TAMPEREEN TEKNILLINEN YLIOPISTO
TAMPERE UNIVERSITY OF TECHNOLOGY

ATTE FINSKA

ESINEIDEN INTERNETIN TIETOTURVAUHAT JA NIIDEN HALLINTAKEINOT

Diplomityö

Tarkastaja: professori Hannu Kärkkäinen
Tarkastaja ja aihe hyväksytty Talouden ja rakentamisen tiedekuntaneuvoston kokouksessa 17.8.2016

TIIVISTELMÄ

ATTE FINSKA: Esineiden internetin tietoturvauhat ja niiden hallintakeinot
Tampereen teknillinen yliopisto
Diplomityö, 75 sivua, 2 liitesivua
Helmikuu 2017
Tietojohtamisen diplomi-insinöörin tutkinto-ohjelma
Pääaine: Tietohallinto ja -järjestelmät
Tarkastaja: professori Hannu Kärkkäinen

Avainsanat: tietoturvallisuus, tietoturva, tietoturvauhka esineiden internet, IoT, tietoturvallisuuden hallinta, riskienhallinta, yksityisyys, teollinen internet

Työn tavoitteena oli lisätä kohdeyrityksen tietoisuutta esineiden internetin tietoturvauhista ja näiden uhkien hallintakeinoista. Kohdeyritys on pohjoismaiden suurin tietoturvakonsultointiin erikoistunut asiantuntijatalo. Tehtävänä oli selvittää mitkä ovat esineiden internetin merkittävimmät tietoturvauhat ja miten näitä uhkia voidaan hallita tehokkaasti. Tietoturvauhkien tunnistaminen ja merkittävyyden pohdinta sekä uhkien hallintaan soveltuvien hallintakeinojen tunnistaminen olivat työssä avainasemassa.

Työn teoria sisältää kaksi osuutta, tietoturvallisuuden hallinnan sekä esineiden internetin tietoturvallisuuden. Teorian keräämisessä aineistona toimi ajankohtaiset ja arvostetut artikkelit sekä perinteisemmän tiedon osalta painettu kirjallisuus. Tietoturvallisuuden hallinnassa korostuu riskienhallinta osana organisaation toimintaa sekä tietoturvauhkien kategorisointi. Esineiden internetin tietoturvallisuuden ymmärtämiseksi esitellään esineiden internetin määritelmä, arkkitehtuuri sekä haasteet, joiden kautta voidaan ymmärtää tietoturvallisuuden tärkeys. Esineiden internetin tietoturvauhkia ja tietoturvallisuuden hallintakeinoja esitellään teorian lopuksi, mutta vasta empiirinen osuus luo työn tärkeimmän sisällön.

Empiirisessä osuudessa haastateltiin tietoturva-asiantuntijoita teemahaastatteluilla, joiden tarkoituksena oli selvittää merkittävimmät tietoturvauhat ja hallintakeinot. Hallintakeinoja lajiteltiin havainnoiviin, suojaaviin sekä estäviin hallintakeinoihin. Tutkimuksen tuloksissa yhdistettiin teorian ja empirian tärkeimmät havainnot, joiden perusteella luotiin merkittävimpien uhkien taulukko sekä merkittävimpien hallintakeinojen taulukko. Edelleen näistä koostettuna sekä pohdinnan tuloksena saatiin yhdisteltyä työn tärkeimpänä tuloksena syntynyt taulukko, joka yhdistää merkittävimmät uhat ja niitä vastaavat hallintakeinot, sekä ottaa kantaa uhan aiheuttamiin seurauksiin sekä tietoturvallisuuden vaarantavaan osa-alueeseen.

ABSTRACT

ATTE FINSKA: Information security threats and management on the Internet of Things
Tampere University of Technology
Master of Science Thesis, 75 pages, 2 Appendix pages
February 2017
Master's Degree Programme in Information and Knowledge Management
Major: Information Management and Systems
Examiner: Professor Hannu Kärkkäinen

Keywords: information security, security threats, information security management, IoT, internet of things, risk management, privacy

The objective of this research was to add knowledge about the information security threats and management on the Internet of Things in the target company. Target company is the biggest information security consulting company in the Nordics. The mission was to identify what are the most significant security threats and how can they be managed effectively on the Internet of Things. Identifying information security threats, significance consideration and identifying proper threat management of these described threats, were the key aspects of this study.

Study's theoretical part consists of two parts, information security management and information security of the Internet of Things. Theory was gathered from current and recognized journals and the more traditional information was obtained from informative books. Risk management as a part of organizations operation and information security threat categorization emphasizes in information security management. To understand the information security aspects of the Internet of Things, the study declares the definition, architecture and challenges of the Internet of Things. Through this the reader can understand the importance of information security. Information security threats and ways to manage them are explained at the end of theory but the empirical part brings out the most important information.

In the empirical part consisted of theme interviews with the information security professionals. The object of the interviews was to define the most significant security threats and ways to manage them. Information security threat management was divided to perceptive, protective and prohibitive management. The study's results combine the most critical observations of the theoretic and the empiric parts. The table of the most significant threats as well as the table of threat management ways were put together from this information. As this was analyzed and taken into consideration the most important result of the study was obtained. A table that combines the information security threats, the possible outcomes of the threat, the information security field that it endangers and lastly the way to manage the said threat.

ALKUSANAT

Kiitos kohdeyritykselle diplomityö mahdollisuudesta, jonka sain toteuttaa täysin oman mielenkiintoni perusteella. Tehtävä osoittautui paljon monimutkaisemmaksi, mitä alkuun ajattelin, mutta nyt paljon aikataulusta jäljessä voin vihdoin todeta työn olevan valmis. Lukuisat päivät ja useat yöt tietokoneen ruutua tuijottaneena, ymmärrän, että tämä on ollut opintojeni vaikein ja rankin osuus, mutta samalla myös opettavaisin. Olen oppinut paljon itsestäni kuin myös aiheesta, joka oli aluksi minulle melko tuntematon.

Kiitokset myös ohjaajalleni Hannu Kärkkäiselle työn varrella tarvitusta tuesta ja opastuksesta. Lisäksi kiitokset koko TTY:lle mahtavista opiskelu vuosista, joita voin hyvällä mielellä muistella lämmöllä vielä pitkään. Opintojen alussa hyvin käsittämättömältä tuntuneet käsitteet ja tietojohtamisen perusopinnot ovat osoittautuneet yritysmaailmassa juuri niiltä asioilta, joita tällä hetkellä arvostetaan. Näin ollen voin olla erittäin tyytyväinen valintaani, joka myös tuntuu omalta.

Loppujen lopuksi koen, että tämän työn tekeminen on valmistanut minua moniin työelämässä vastaan tuleviin haasteisiin, jotka osaan nyt ottaa vastaan paremmin kuin ennen työn tekemistä. Yleispätevät ominaisuudet, kuten ajanhallinta ja asioiden priorisointi ovat tulleet hyvinkin tutuiksi työn kirjoittamisen aikana. Uskon, että näiden oppien myötä olen valmis kohtaamaan tulevaisuuden haasteet reppu täynnä muistoja, kokemuksia sekä tärkeitä oppeja elämään.

Helsingissä, 13.2.2017

Atte Finska

SISÄLLYSLUETTELO

1. JOHDANTO

Tietoturvallisuuden merkitys kasvaa jatkuvasti digitalisaation ja tiedon lisääntymisen myötä. Tiedon arvo yrityksille on mittaamattoman arvokasta, minkä takia sen turvaamiseksi ollaan valmiita käyttämään resursseja kasvavalla tahdilla. Tietoa on nykyään kaikkialla, hiljaisena tietona työntekijöissä ja tallennettuna kaikissa tietojärjestelmissä. Näiden turvallisuus on noussut uutisotsikoihin entistä vahvemmin viimeisten vuosikymmenten aikana. Digitalisaatio on mahdollistanut entistä nopeamman tiedon vaihdon ja helpottanut tiedon luomista, käyttöä ja tallentamista. Kaikkea tätä tietoa tulee turvata, ettei tieto vuoda asiattomien käsiin.

Esineiden internet on jo vanha käsite, mutta vasta viime vuosina sitä on alettu pitää konkreettisesti merkittävänä ilmiönä. Esineiden internet koostuu fyysisistä laitteista, jotka seuraavat ympäristöään ja pystyvät tämän perusteella toimimaan älykkäästi ja kommunikoimaan muiden laitteiden kanssa. Esineiden internet perustuu datan keräämiseen, sen käyttämiseen ja analysointiin päätöksenteon tukena. Esineiden internet liittyy vahvasti digitalisaatioon ja tarkoittaa käytännössä erilaisten sensorien muodostaman verkoston liittämistä osaksi suurempia tietojärjestelmiä. Tämän tutkimuksen kannalta sensoreita ovat älyautot, jotka automaattisesti keräävät dataa auton toiminnasta sekä sen ympäristöstä. Kerätty data siirretään automaattisesti datayhteyksien kautta palvelimille, jonne se tallennetaan. Tallennettua dataa analysoidaan, minkä perusteella voidaan esimerkiksi ennustaa, milloin auto tulisi viedä huoltoon. Kerätty data on monessa tapauksessa hyvin sensitiivistä ja arvokasta, minkä takia tietoturvallisuus on huomioon otettava osa esineiden internetiä. Älyauton tapauksessa tietoturvallisuus on noussut uutisotsikoihin, kun hakkerit onnistuivat kytkemään auton jarrut pois käytöstä.

Esineiden internetin tietoturvallisuus nousee vahvasti esille puhuttaessa linkitetyistä laitteista, jotka keräävät dataa esimerkiksi kuluttajan sähkönkäytöstä. Tätä dataa hyväksi käyttämällä pystytään analysoimaan kuluttajan toimintaa ja jopa päättelemään hänen liikkumisiaan ja tottumuksiaan. Ulkopuolisen henkilön käsissä datan perusteella voidaan jopa päätellä, milloin kuluttaja on pois kodistaan tai esimerkiksi lomamatkalla. Toinen esimerkki energiateollisuudesta on vuosi sitten uutisissa ollut Ukrainan sähköverkon kaataminen (Halminen 2016). Tapauksessa sähköyhtiön järjestelmiin oli päässyt haittaohjelma Blackenergy, joka on suunniteltu korruptoimaan käyttöjärjestelmälle tärkeitä ohjelmatiedostoja. Haittaohjelma onnistui katkaisemaan sähköt noin puolilta ukrainalaisen kaupungin Ivano-Frankivskin asukkaista, mikä tarkoitti noin 700 000 kotitaloutta. Tämä oli tiedettävästi ensimmäinen kerta, kun haittaohjelman avulla on saatu katkaistua sähkönjakelu kuluttajilta. Teollisuuden hallintajärjestelmät, mukaan lukien teollisuus automaatio (esineiden internet) ovat olleet hyökkäyksien kohteena aiemmin-

kin, mutta viimeistään nyt hyökkäyksiin tulee suhtautua vakavasti. Kriittisen infrastruktuurin turvaamiseen tulee kiinnittää huomiota, sillä tämän kaltaisia tapauksia on osattu jo odottaa, mutta nyt niistä on myös konkreettista näyttöä.

Tässä tutkimuksessa perehdytään esineiden internetin tietoturvauhkiin ja näiden uhkien hallintakeinoihin. Tutkimusta konkretisoi älyauton tietoturvan pitäminen esimerkkinä, jolloin uhkia ja hallintakeinoja peilataan sitä vasten. Älyautoa itseään ei tutkimuksessa varsinaisesti tutkita, vaan se toimii lähinnä konkreettisena esimerkkinä, havainnollistamaan yhden tartuntapinnan esineiden internetin tietoturvallisuudelle.

1.1 Tutkimuksen tausta

Tutkimus toteutetaan tilauksena asiakasorganisaatiolle, joka on suomalainen kyberturvallisuusalan yritys. Yritys toimii laajasti kaikilla kyberturvallisuuden osa-alueilla toimittaen asiakkailleen ratkaisuja tietoturvallisuuden suunnittelusta aina toteutukseen asti. Yritys on pohjoismaiden suurin tietoturvakonsultointiin erikoistunut asiantuntijaorganisaatio. Kooltaan yritys lukeutuu pk-yrityksiin ja kasvaa nopealla tahdilla. Kansainvälistyminen on aloitettu vuoden 2015 loppupuolella ja on osa pitkän aikavälin strategiaa.

Tutkimuksen taustalla on yrityksen ilmaisema kiinnostus oppia lisää esineiden internetin tietoturvallisuudesta ja sen hallinnasta. Tutkimus käsittelee tietoturvauhkia ja uhkien hallintaa esineiden internetissä. Tutkimus ei tule ratkaisemaan mitään suoranaista ongelmaa, vaan tulee toimimaan yrityksen oppimisen apuna ja tulevaisuudessa mahdollisesti myös työkaluna konsultoinnissa.

Tavoitteena tutkimuksessa on tunnistaa kattavasti esineiden internetin tietoturvauhkia, arvioida mitkä uhat ovat merkittävimpiä ja etsiä näille uhille tehokkaita hallintakeinoja. Tuloksissa esitellään merkittävimmät uhat ja niitä vastaavat hallintakeinot, jotka pyritään pitämään mahdollisimman konkreettisina, jotta työn tuloksia voidaan hyödyntää yrityksessä myös jatkossa.

Tutkimuksen tarkoitus on olla korkeamman tason kuvaus siitä, millaisia tietoturvauhkia esineiden internetiin liittyy ja miten niistä merkittävimpiä voidaan hallita. Tavoitteena on, että yritys pystyy tulevissa asiakasprojekteissa hyödyntämään tutkimuksen tuloksien listaa tärkeimmistä uhista ja nopeasti toteamaan, miten listan uhkia voidaan hallita tehokkaasti. Listan perusteella yritys voi tunnistaa yleisimpiä esineiden internetin tietoturvauhkia, joiden perusteella tarjotaan asiakkaille niiden hallintaan soveltuvia palveluita.

Esineiden internet on hyvin laaja käsite, kuten myös tietoturvallisuus, mikä luo haasteen tutkimuksen kirjoittajalle. Aihealueen ollessa kahden laajan kokonaisuuden yhdistelmä, ei kaikkia aihealueiden osa-alueita voida käydä läpi tutkimuksen asettamissa rajoissa. Tutkimuksen tavoitteena on olla ylemmän tason kuvaus esineiden internetin tietoturval-

lisuudesta, jota on lähestytty konkreettisen esimerkin avulla. Saatuja tuloksia pyritään yleistämään myös muille osa-alueille mahdollisuuksien mukaan. Haasteena tutkimuksessa on, että tietoturvauhat vaihtelevat merkittävästi riippuen puhutaanko terveydenhuollon palveluista tai sovelluksista vai esimerkiksi valitusta älyautosta.

Kohdeyritys voi käyttää jatkossa tutkimuksen tuloksia asiakasprojekteissa konsultoinnin työkaluna esineiden internetiin liittyvissä projekteissa uhkien tunnistamiseen, määrittelyyn ja hallintakeinojen suunnittelun apuvälineenä. Tuloksista voidaan jälkikäteen koostaa lyhyt checklist tyypinen ratkaisu, jota on helppoa ja nopeaa käyttää apuna konsulttien kiireisessä työympäristössä.

1.2 Tutkimuskysymykset, tutkimuksen näkökulma ja rajaus

Tutkimuksen tavoitteena on luoda ymmärtävä selvitys esineiden internetin tietoturvauhista ja niiden hallintakeinoista.

Tutkimuksen päätutkimuskysymys on:

- Miten esineiden internetin tietoturvauhkia voidaan hallita tehokkaasti?

Päätutkimuskysymystä tukemaan on tunnistettu seuraavat ongelman pienempiin osiin jakavat alatutkimuskysymykset:

- Mitä tietoturvauhkia esineiden internetiin liittyy?
- Mitkä tietoturvauhat ovat merkittävimpiä esineiden internetissä?
- Millaisilla hallintakeinoilla esineiden internetin tietoturvauhkia voidaan hallita tehokkaasti?

Näkökulma tutkimuksessa on tutkia tietoturvan osuutta esineiden internetissä, millaisia uhkia tietoturvallisuudelle on ja millaisilla keinoilla uhkia voidaan hallita. Näkökulma huomioi uhat esineiden internetin arkkitehtuurin eri tasoilla ja tarkastelee näitä uhkia vastaavia hallintakeinoja. Empirian yhtenä osana peilataan esineiden internetin tietoturvallisuutta älyautoon konkreettisena esineiden internetin sovelluksena.

Tutkimus rajataan tiettyihin aiheiden osa-alueisiin, sillä aihealueet ovat sen verran laajoja, että muutoin työn pituus ylittäisi diplomityön sallitut rajat. Rajaukset on tehty yhteistyössä tutkimukseen osallistuvien osapuolten kanssa.

- Esineiden internetin osalta käytetään arkkitehtuurin kolmeen tasoon jakavaa mallia (havainnointitaso, siirtotaso, sovellustaso)
- Tietoturvallisuuden osalta käsitellään tietoriskejä, tietoturvariskejä sekä tietosuojaa ja näihin liittyviä hallintakeinoja
- Työssä tarkastellaan tilannetta työn tilaajaorganisaation asiakkaan näkökulmasta, joka on lähes poikkeuksetta toinen yritys.

Rajaukset auttavat pitämään työn sen sallituissa mitoissa sekä tutkijaa selventämään aihealueiden laajuutta. Rajausten avulla myös tutkimuksen aihe pysyy tarkkana eikä lähde rönsyilemään aiheen ulkopuolelle.

1.3 Tutkimusmetodologia

Tämä tutkimus toteutetaan ymmärtävänä kvalitatiivisena tutkimuksena. Tutkimus tulee koostumaan teoreettisesta sekä empiirisestä osiosta. Teoreettinen osio luo viitekehyksen tietoturvallisuudelle, esineiden internetille sekä esineiden internetin tietoturvallisuuden hallinnalle. Empiirisessä osiossa tutkitaan yleisesti esineiden internetin tietoturvallisuutta, sen uhkia sekä tietoturvallisuuden hallintakeinoja. Lisäksi empiriassa tutkitaan älyauton tietoturvallisuutta teemahaastatteluiden avulla, joissa aihealue selitetään haastateltaville.

Tässä tutkimuksessa empirian keräämisen muodoksi valittiin puolistrukturoidut teemahaastattelut. Haastatteluiden tavoitteena on saada lisää ymmärrystä esineiden internetin tietoturvasta, tietoturvauhista ja uhkien hallintakeinoista. Haastatteluiden kysymysrunko suunnitellaan ja toteutetaan siten, että näkökulmat määritellään ennalta, säilyttäen pieni vapaus haastattelun etenemiselle muihinkin suuntiin. Haastateltavilta on tavoitteena saada tietoa olemassa olevista tietoturvauhista esineiden internetissä sekä erityisesti uhkien konkreettisista hallintakeinoista. Tutkimuksen metodologia on esitetty alla olevassa taulukossa 1.

Taulukko 1.1. *Tutkimuksen metodologia*

Tutkimusfilosofia	Hermeneutiikka
Tutkimuksen suuntaus	Deduktiivinen
Tutkimusmenetelmä	Kuvaileva tapaustutkimus (teoriaa testaava case-tutkimus, Lukka 1999)
Tiedonkeruumenetelmät	Kirjallisuus, teemahaastattelut
Tutkimustyyppi	Kvalitatiivinen

Olkkonen (1994) määrittelee tärkeimmiksi tieteenkäsityksiksi positivismin ja hermeneutiikan. Positivismi on tieteenkäsitys, joka perustuu ajatukseen, että tutkimus on tekijästä riippumaton ja toistettavissa oleva. Positivismin perusajatuksena on, että tieto perustuu todennettuihin tosiasioihin, esimerkiksi mittaustuloksiin. Hermeneutiikka puolestaan ei takaa riippumattomuutta, sillä se tukeutuu tutkijan ymmärrykseen aineistosta.

Aineisto on useimmiten kvalitatiivista, mikä soveltuu tähän tutkimukseen kvalitatiivisuuden myötä.

Tutkimuksen suuntauksia ovat deduktiivinen ja induktiivinen päättely (Olkkonen 1994). Deduktiivinen päättely tarkoittaa, että yleisistä väitteistä kootaan erikoisempia päätelmiä. Vastaavasti induktiivinen päättely lähtee liikkeelle erikoisemmista väitteistä, jotka liitetään yleiseksi väitteeksi. Tämän tutkimuksen kannalta deduktiivinen päättely on luontevampaa, sillä tietoturvallisuudesta ja teollisesta internetistä kootaan yleisiä asioita, jotka kootaan yhtenäiseksi kokonaisuudeksi. Deduktiivinen päättely sopii myös pohjimmiltaan teoreettiseen tutkimukseen, missä totena pidetyistä väitteistä johdetaan yksityistapausta koskeva sovellutus.

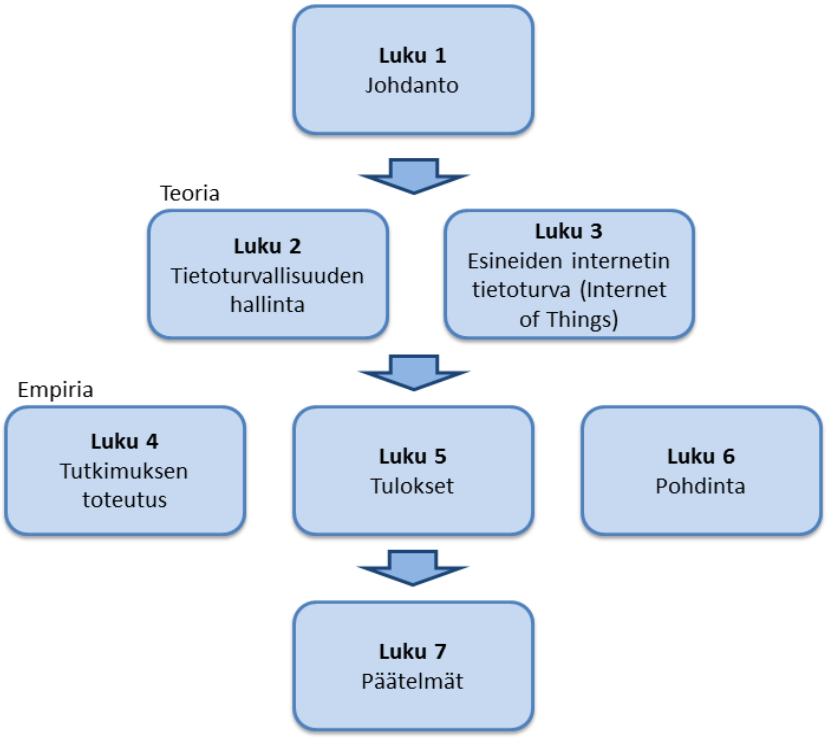
Tutkimusmenetelmäksi valittiin tapaustutkimus, sillä tutkimukseen liittyy tietty yksityiskohtainen tapaus, jota tarkastellaan yksityiskohtaisemmin teoriaan liittäen. Tässä tutkimuksessa perehdytään älyautoon ja sen toimintaan osana suurempaa esineiden internetin järjestelmää. Tapaustutkimuksella pyritään kokonaisvaltaiseen ymmärrykseen asiasta, mikä kuvaa hyvin tätä tutkimusta. Tästä voidaan tarkentaa tapaustutkimusta edelleen kuvailevaksi tapaustutkimukseksi. Kuvaileva tapaustutkimus pyrkii kuvaamaan tarkasteltavaa ilmiötä mahdollisimman yksityiskohtaisesti, laajasti ja kaiken huomioiden. Tässä on kuitenkin muistettava tutkimuksen rajaukset, mitkä rajaavat tutkimuksen vain tiettyihin tietoturvallisuuden ja esineiden internetin osa-alueisiin.

Tiedonkeruumenetelminä tässä tutkimuksessa toimivat kirjallisuuskatsaus sekä teemahaastattelut. Kirjallisuuskatsaus tarkastelee tutkimukseen liittyviä näkökulmia, teorioita ja aiempia julkaisuja. Näiden perusteella voidaan koota teoreettinen viitekehys tutkimukselle, joten kirjallisuuskatsaus toimii teoreettisen osuuden tiedonkeruumenetelmänä. Empiirisessä osiossa tarkastellaan yksityiskohtaista rajattua aihetta, joten siihen soveltuu asiantuntijoille tehtävät teemahaastattelut. Teemahaastattelut suunnitellaan etukäteen ja pyritään pitämään mahdollisimman objektiivisina, jotta saadut tulokset olisivat mahdollisimman todenmukaisia. Haastattelut toteutetaan puolistrukturoituina, sillä haastatteluissa halutaan saada yksityiskohtaista tietoa määrätyistä teemoista, eikä haastateltaville haluta antaa liikaa vapauksia (Saaranen-Kauppinen & Puusniekka 2006).

Edellä mainittujen valintojen perusteella voidaan tutkimuksen sanoa olevan kvalitatiivinen eli laadullinen tutkimus. Tutkimus pyrkii ymmärtämään aihetta kokonaisvaltaisesti ja syventymään empirian osalta määriteltyyn rajattuun aiheeseen. Teoriaa käytetään keinona, jolloin empirian tuloksia arvioidaan teoriaa vastaan ja näin pyritään rakentamaan ymmärtävä kuvaus esineiden internetin tietoturvauhista ja niiden hallintakeinoista. Tutkimuksen lopputuloksena syntyy listaus merkittävimmistä esineiden internetin tietoturvauhista sekä näitä vastaavista hallintakeinoista.

1.4 Tutkimuksen rakenne

Tutkimus voidaan jakaa karkeasti kahteen osaan, teoreettiseen ja empiiriseen. Tutkimuksen rakenne koostuu johdannosta, teoreettisesta kirjallisuuskatsauksesta, empiirisestä tutkimuksesta, tuloksista, pohdinnasta sekä päätelmistä. Johdannossa esitellään aihealuetta, käydään läpi tutkimusongelmat, tavoitteet sekä tutkimukseen liittyvät valinnat. Valinnat sisältävät tutkimuksen näkökulman ja tutkimusmetodologian läpikäymisen. Tutkimusmetodologia ohjaa tutkimuksen tekemistä ja arviointia.



Kuva 1.1. *Tutkimuksen rakenne*

Kirjallisuuskatsauksessa esitellään tutkimuskysymyksiin liittyvä teoria kokonaisvaltaisesti. Teoria jakaantuu edelleen kahteen osaan, tietoturvallisuuden hallintaan ja esineiden internetin tietoturvallisuuteen. Ensimmäinen osio kuvaa tietoturvallisuutta ja sen hallintaa yleisellä tasolla sekä kuvaa tietoturvallisuuden osa-alueita ja ulottuvuuksia. Lisäksi esitellään, kuinka tietoturvallisuus liittyy organisaation liiketoimintaan ja miten riskienhallinta liittyy tähän tutkimukseen. Lopuksi esitellään tietoturvauhkien kategorisointia. Toisessa osiossa perehdytään esineiden internetiin, sen määritelmiin, arkkitehtuuriin, haasteisiin, ominaisuuksiin ja tietoturvallisuuteen. Osiossa kuvataan myös esineiden internetin osa-alueita sekä haasteita. Lisäksi osiossa tarkastellaan tietoturvallisuuden ja esineiden internetin liittymistä toisiinsa sekä tähän liittyviä uhkia ja uhkien hallintakeinoja. Kirjallisuuskatsauksessa tavoitteena on luoda teoreettinen pohja tutkimuksen empiiriselle osalle. Tietoa on haettu pääsääntöisesti sähköisistä artikkeleista,

mutta jonkin verran myös painetusta kirjallisuudesta. Painettu kirjallisuus painottuu tietoturvallisuuden yleiseen kuvaukseen, kun taas sähköiset artikkelit käsittelevät pääsääntöisesti enemmän esineiden internetiä.

Empiirinen osuus koostuu viiden asiantuntijan teemahaastattelusta sekä yhdestä tilaajaorganisaation ulkopuolisesta haastattelusta. Tavoitteena haastatteluissa on tunnistaa tietoturvauhkia, määrittää näistä merkittävimmät sekä etsiä merkittävimmille uhille hallintakeinoja. Haastatteluiden tavoitteet ovat melko korkealla, mikä saattaa muodostua ongelmaksi tulosten kannalta. Älyautoa käytetään haastatteluissa konkretisoimaan esineiden internetin osa-aluetta ja siihen liittyvää tietoturvallisuutta. Haastatteluissa tunnistetuista uhista pyritään koostamaan taulukko, josta lukijalle selviää esineiden internetin merkittävimmät tietoturvauhat ja näiden hallintakeinot.

Tuloksissa kerätään yhteen havaitut tietoturvauhat ja avataan niitä hieman enemmän. Löydettyjä uhkia pyritään hallitsemaan niitä vastaavilla hallintakeinoilla, jolloin uhat liitetään hallintakeinoihin. Tuloksena saadaan täten taulukko esineiden internetin merkittävimmistä tietoturvauhista, johon liitetään osaksi uhkia vastaavat hallintakeinot sekä tietoturvallisuuden vaarantava osa-alue. Pohdinnassa analysoidaan tutkimuksen tuloksia eritellen ensin tunnistettuja uhkia, jonka jälkeen analysoidaan uhkien hallintakeinoja. Pohdinnassa otetaan myös kantaa merkittävimpiin tuloksiin ja pohditaan niiden paikkansa pitävyyttä sekä syitä.

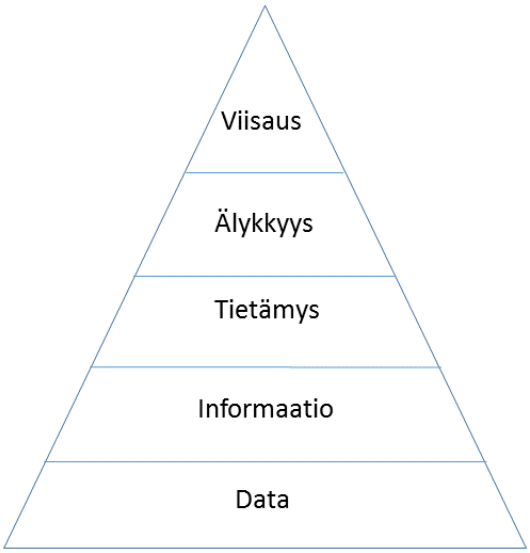
Lopuksi tutkimuksen tulokset kootaan yhteen ja vedetään niistä johtopäätökset. Tutkimusta ja tuloksia arvioidaan ja verrataan aluksi asetettuihin tavoitteisiin. Viimeiseksi esitetään mahdollisia jatkotutkimusehdotuksia.

2. TIETOTURVALLISUUDEN HALLINTA

Tässä luvussa perehdytään tietoturvallisuuteen käsitteenä ja ilmiönä. Seuraavaksi tarkastellaan sen osa-alueita sekä liittymistä organisaation toimintaan. Lopuksi tutustutaan riskienhallintaan sekä tietoturvauhkien kategorisointiin.

2.1 Tieto ja turvallisuus

Tietoturvallisuus koostuu terminä kahdesta osasta: tiedosta ja turvallisuudesta. Tieto on sanakirjan mukaan dataa, informaatiota, opittua tietämystä, viisautta, ilmoitus, todellisuuteen perustuva käsitys jostakin, tosiasioiden tuntemista tai tietoisuutta (Sivistyssanakirja 2015). Tieto jaetaan perinteisesti kolmeen perustasoon: dataan, informaatioon ja tietämykseen (Liebowitz 2006; Thierauf 2001; Sydänmaanlakka 2007). Sydänmaanlakka (2007) lisää edellä mainittuihin tasoihin vielä älykkyyden ja viisauden. Nämä tiedon tasot on esitetty kuvassa 2.1, missä tieto on alimmalla tasolla dataa ja ylimmällä tasolla viisautta.



Kuva 2.1. *Tiedon tasot (Mukailtu lähteestä Liebowitz 2006)*

Tiedon hierarkiassa alimmalla tasolla on data. Data on numeroita, tekstiä, kuvia, merkkejä tai näiden yhdistelmä, jolla ei itsessään ole merkitystä (Kaario & Peltola 2008, s. 6; Ståhle & Grönroos 1999, s. 207). Erilaisilla muunnosprosesseilla datasta voidaan muokata informaatiota (Hakala 2006, s. 66; Sydänmaanlakka 2007, s. 187). Esimerkkejä tällaisista muunnoksista ovat jäsentely, liittäminen, korjaaminen, analysointi ja tiivistäminen (Liebowitz 2006, s. 7; Sydänmaanlakka 2007, s. 188). Informaatiolla on jokin

merkitys vastaanottajalle. Informaatio on dataa jossain tietyssä kontekstissa, jolloin sillä on jonkinlainen informaatioarvo vastaanottajalle (Kaario & Peltola 2008, s. 6; Liebowitz 2006, s. 7; Ståhle & Grönroos 1999, s. 49). Kolmannella tasolla kuvassa 2.1 on tietämys, joka sisältää informaation vaikutuksen ja on täten muuttunut inhimilliseksi tiedoksi, jota voidaan hyödyntää jonkin ongelman ratkaisemiseksi tai tehtävän suorittamiseksi (Ståhle & Grönroos 1999, s. 49). Ylimmät kaksi tiedon tasoa liittyvät vahvasti henkilöön ja hänen asiantuntijuuteensa sekä kokemukseen. Nonaka & Takeuchi (1995) jakavat tiedon hiljaiseen ja eksplisiittiseen tietoon. Hiljainen tieto on vaikeasti nähtävää ja ilmaistavaa, se on yksilöihin sitoutunutta, kokemuksen kautta opittua tietoa, jonka avulla voidaan luoda eksplisiittistä tietoa, vaikka sen siirtäminen onkin haastavaa. Eksplisiittistä tietoa voidaan ilmaista numeroilla tai sanoilla ja se on formaalia sekä systemaattista tietoa, jota on helppoa jakaa. (Nonaka & Takeuchi 1995, s. 8) Molempien sekä hiljaisen että eksplisiittisen tiedon jakaminen on organisaation edun mukaista, mutta se ei saa olla ristiriidassa tietoturvallisuuden kanssa.

Turvallisuus on Merriam-Webster sanakirjan mukaan ”ominaisuus tai tila, jossa koetaan 1) vapaus vaarasta 2) vapaus pelosta tai huolesta 3) vapaus mahdollisuudesta tulla irtisanotuksi. Turvallisuus voi olla myös toimenpiteitä, joilla suojaudutaan esimerkiksi vakoilulta, sabotoinnilta, rikoksilta, hyökkäyksiltä tai pakenemiselta.

Tiedosta ja turvallisuudesta muodostuva termi, tietoturvallisuus, on siis jotain tiedon turvaamiseksi tehtäviä toimenpiteitä. Usein tietoturvallisuus koetaan tekniseksi asiaksi, vaikka todellisuudessa tietoturvallisuus on sekä hallinnollisia että teknisiä ratkaisuja. Organisaatiossa tietoa on muun muassa tallennettuna datana tietojärjestelmissä ja ihmisiin liittyneenä tietämyksenä. Kyrölän (2001) mukaan tietoturvallisuudessa kahdeksankymmentä prosenttia toiminnasta on hallinnollista, mikä käsittää ihmisten toiminnan, päätöksenteon ja muita inhimillisiä asioita. Hän sanoo, että vain loput kaksikymmentäprosenttia ovat teknisiä ratkaisuja, mikä korjaa yleisesti vallitsevaa epäymmärrystä.

Tietoturvallisuus tarkoittaa eri tiedon tasoilla erilaisia ratkaisuja. Mitä alemmalle tiedon tasolle siirrytään, sitä teknisemmiksi tietoturvallisuuden ratkaisut muuttuvat. Ylemmillä tasoilla tieto muuttuu konteksti- ja ihmisriippuvaiseksi, jolloin tekniset ratkaisut eivät toimi. Ylempien tasojen tietoturvallisuus koostuu ihmisten kouluttamisesta ja toiminnan muokkaamisesta tietoturvallisemmaksi. Ylemmillä tasoilla tieto on arvokkaampaa, jolloin sen turvaamiseen on liiketoiminnallisesti järkevää panostaa enemmän. Ylemmillä tasoilla tietoturvallisuus on enemmän hallinnollisia ratkaisuja, mikä on linjassa Kyrölän (2001) kanssa. Alemmilla tasoilla tieto ei itsessään ole välttämättä yhtä arvokasta ja ratkaisuina toimii monenlaiset tekniset järjestelmät ja suojaustavat.

Peltier et al. (2005, s. 1) mukaan tietoturvallisuuden tarkoitus on suojata organisaation arvokkaita resursseja eli tietoja, laitteistoja ja ohjelmistoja. Whitman & Mattord (2005, s. 37-38) puolestaan pitävät tietoturvallisuuden tavoitteena organisaation toimintakyvyn varmistamista, joka koostuu sovelluksista, datasta ja teknisistä resursseita. Käytännön

tasolla tietoturvallisuudella suojellaan koko organisaation toimintaa, kattaen kaikki osa-alueet.

2.2 Tietoturvallisuuden osa-alueet ja ulottuvuudet

Tietoturvallisuus voidaan jakaa osa-alueisiin osana organisaation toimintaa sekä tiedon arvoa tuottavien ominaisuuksien näkökulmasta. (Tipton & Krause 2004; Whitman & Mattord 2005). Tietoturvallisuuden moninaisuuden ja kompleksisuuden vuoksi tapoja aiheen jaotteluun on useita. Perinteinen jaottelu on ISO/IEC 27001 –standardin mukainen tapa, jota muun muassa Tipton & Krause (2004) ja Whitman & Mattord (2005) käyttävät tietoturvallisuutta käsitellessään. Valtionhallinto käyttää samankaltaista jaottelua julkaisemissaan ohjeistuksissa ja tietoturvallisuuden osa-aluejaossaan. Taulukossa 2.1 esitellään perinteinen ja yleisesti tunnettu kahdeksanosainen jaottelu. Taulukossa esitellään lyhyesti jokaisen osa-alueen tavoitteet ja annetaan muutama esimerkki konkreettisista osa-alueeseen liittyvistä tietoturvatoiminnoista. Tietoturvatoiminnoilla tarkoitetaan konkreettisia toimia organisaation tietoturvallisuuden ylläpitämiseksi. Näillä toiminnoilla pyritään estämään epäsuotuisten ja haitallisten tapahtumien realisoitumista. Esimerkkinä tietojen vuotaminen organisaation ulkopuolelle tai tietojärjestelmien väärinkäytökset.

Taulukko 2.1. *Tietoturvallisuuden osa-alueet (Mukailtu lähteistä VAHTI & ISO/IEC 27001)*

Henkilöstöturvallisuus **Tavoite**: Henkilöistä aiheutuvien riskien pienentäminen, tiedon suojaaminen ja saatavuuden turvaaminen **Esimerkki toimintoja**: Henkilöstön kouluttaminen, tehtävien eriyttäminen	**Hallinnollinen turvallisuus** - Tietoturvapolitiikka - Johdon sitoutuminen - Riskienhallinta - Sopimukset - Jatkuvuuden suunnittelu - Organisointi ja vastuu - Henkilöstön koulutus - Tietojen luokittelu
Tietoaineistoturvallisuus **Tavoite**: Tietoaineistojen riittävän suojauksen varmistaminen **Esimerkki toimintoja**: Tietoaineiston käsittelysäännöt, luokittelu, luettelointi, henkilöstön perehdyttäminen	
Fyysinen turvallisuus **Tavoite**: Organisaation häiriöttömän toiminnan turvaaminen kaikissa olosuhteissa, toimitilojen ja tietoaineistojen turvaaminen luvattomalta tunkeutumiselta **Esimerkki toimintoja**: Kulunvalvonta, vartiointi, palovahinkojen torjunta	
Ohjelmistoturvallisuus **Tavoite**: Ohjelmistojen turvallinen käyttö ja tiedon eheyden säilyminen **Esimerkki toimintoja**: Ohjelmistokehityksen prosessit, valvontalokit, päivitykset	
Tietoliikenneturvallisuus **Tavoite**: Tietoliikenteen ja sitä tukevan arkkitehtuurin suojaaminen **Esimerkki toimintoja**: Lokit, verkon hallinta, verkon segmentointi, tietoliikenteen	

salaus	
Laitteistoturvallisuus **Tavoite**: Laitteiden elinkaaren turvaaminen, omaisuuden häviämisen, vahingoittumisen, varkauksien estäminen **Esimerkki toimintoja**: Laitteiden sijoitus, suojaus, valvonta ja ylläpito	
Käyttöturvallisuus **Tavoite**: Luoda ja ylläpitää tietotekniikan turvallisia toimintaolosuhteita **Esimerkki toimintoja**: Käyttöoikeuksien hallinta, varmuuskopiointi, tietojen luokittelu, järjestelmien ylläpito	

Tietoturvallisuus voidaan jakaa kolmeen perusulottuvuuteen, joita ovat luottamuksellisuus, eheys ja saatavuus (Brotby 2009; Peltier et al. 2005; Tipton & Krause 2004; Whitman & Mattord 2005; ISO/IEC 27001:fi). Näiden avulla tietoturvallisuus myös perinteisesti määritellään. Luottamuksellisuudella tarkoitetaan tietojen säilymistä luottamuksellisina ja tietoihin jaettujen oikeuksien oikeanlaista käsittelyä. Eheydellä viitataan tietojen sisäiseen ristiriidattomuuteen, kattavuuteen, ajantasaisuuteen, oikeellisuuteen ja käyttökelpoistuuteen. Eheydelle ominaista on, että tietoa ei ole valtuudettomasti muutettu ja että mahdolliset muutokset voidaan todentaa. Saatavuus viittaa ominaisuuteen, että tieto, järjestelmä tai palvelu on saatavilla siihen oikeutetuille haluttuna aikana vaadittavalla tavalla. (VAHTI 8/2008)

Luottamuksellisuus, kuten kaikki muutkin tietoturvallisuuden ulottuvuudet, riippuvat toisistaan. Luottamuksellisuus liittyy kaikkein lähimmin yksityisyyteen, jolla tarkoitetaan yksityishenkilöiden, työntekijöiden, asiakkaiden tai potilaiden henkilökohtaisia tietoja (Whitman & Mattord 2005, s.11-12). Henkilökohtaisia tietoja ovat esimerkiksi nimi, osoite ja luottokorttitiedot. Whitman & Mattord (2005, s. 11-12) mukaan luottamuksellisuutta voidaan turvata esimerkiksi tiedon luokittelulla, turvallisella dokumenttien säilyttämisellä, yleisten turvallisuus käytäntöjen käyttöönotolla sekä käyttäjien koulutuksella. ISO/IEC 17799 –standardin mukaan luottamuksellisuus tarkoittaa tiedon saatavuuden varmistamista vain niille, joilla on valtuutettu lupa siihen.

Eheys on määritelty ISO/IEC 17799 –standardissa toimiksi tiedon tarkkuuden, täydellisyyden ja prosessoinnin tapojen turvaamiseksi. Whitman & Mattrod (2005, s. 12) sanovat tiedon olevan eheää, kun se on kokonaista, täydellistä ja korruptoitumatonta. Tiedon eheys on vaarassa, mikäli tiedon alkuperäistä muotoa korruptoidaan, vahingoitetaan, tuhotaan tai muutoin muunnellaan. Eheys voi rikkoontua tietoa tallennettaessa tai lähetettäessä. Eheyden varmistamiseksi voidaan käyttää erilaisia tarkistuslukuja ja tiivisteitä, joiden perusteella voidaan päätellä, onko tieto pysynyt muuttumattomana.

Saatavuus mahdollistaa vaadittuna ajankohtana esteettömän pääsyn tietoon, joka on oikeassa muodossa, niille joilla on siihen valtuutettu lupa (Whitman & Mattord 2005,

s.10). Saatavuutta voidaan ylläpitää esimerkiksi varmuuskopioiden avulla sekä varautumalla palvelunestohyökkäyksiin esimerkiksi skaalautuvuudella. Saatavuus liittyy eheyteen, sillä saatavilla olevan tiedon tulee olla oikeassa muodossa, jotta sitä voidaan käyttää. Myös luottamuksellisuus liittyy saatavuuteen, sillä erittäin salaiset, korkean luottamuksellisuuden dokumentit tulee salata hyvin, jolloin niiden saatavuus pienenee.

Kirjallisuudesta löytyy myös muita tietoturvallisuuden ulottuvuuksia, kuten oikeellisuus, aitous, käytettävyys, hallussapito, tilivelvollisuus, tunnistettavuus ja kiistämättömyys (Brotby 2009; Miettinen 1999; Tipton & Krause 2004; Whitman & Mattord 2005). Suurin osa edellä mainituista ulottuvuuksista laajentaa tai tarkentaa kolmea tietoturvallisuuden pääulottuvuuksista. Kiistämättömyys laajentaa luottamuksellisuutta ja valtionhallinto on määritellyt sen näytöksi, että tietty henkilö on lähettänyt tai vastaanottanut tietyn viestin tai että viesti tai tapahtuman on jätetty käsiteltäväksi (VAHTI 8/2008). Eheyttä täydentävät esimerkiksi aitous, jolla tunnistetaan luotettavasti viestin lähettäjä tai tiedon alkuperä, sekä oikeellisuus, joka nimensä mukaisesti viittaa tiedon virheettömyyteen. Saatavuutta tarkentaa käytettävyys, jolla viitataan ominaisuuteen, miten järjestelmä, laite, ohjelma tai palvelu soveltuu suunniteltuun käyttöön määrätylle kohderyhmälle. (VAHTI 8/2008)

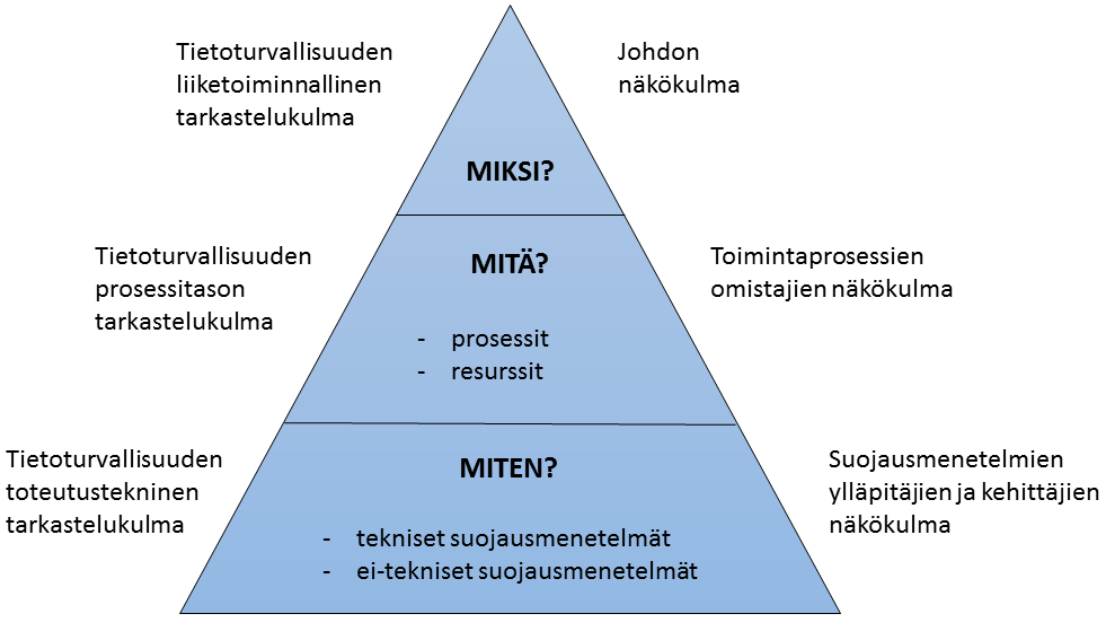
2.3 Tietoturvallisuus osana organisaation toimintaa

Tietoturvallisuuden tavoitteena organisaation toiminnassa on varmistaa organisaation toimintakyky, mahdollistaa turvallinen sovellusta käyttö, suojata organisaation keräämät ja käyttämät tiedot ja suojella teknisiä resursseja (Whitman & Mattord 2005, s. 37). Organisaation toimintakyvyn varmistaminen on pitkälti hallinnollisia toimintoja, ennemmin kuin teknisiä ratkaisuja. Ihmisten toiminta on usein yksi suurin tekijä tietoturvallisuuden lisäämiseksi. Ihmisten tekemät inhimilliset virheet, huolimaton järjestelmien käyttö ja tietämättömyys tietoturvallisuudesta ovat asioita, joihin tietoturvatyössä tulisi keskittyä. Sovellusten käyttö organisaatioissa on usein välttämätön osa työskentelyä, minkä vuoksi sovellusten käytön tulisi olla turvallista ja niiden tulisi olla käytettävissä tarvittaessa. Esimerkiksi käyttöjärjestelmien, sähköpostin ja pikaviestintävälineiden saatavuus vaikuttaa suuresti organisaation liiketoimintaan. Tiedot organisaatioiden järjestelmissä ovat usein erittäin kriittisiä liiketoiminnan kannalta. Tietojen tuhoutuminen, muuttuminen ja paljastuminen ovat suuria uhkia organisaatioiden toiminnalle, minkä vuoksi niiden suojaaminen on tärkeää. Järjestelmissä tallennettuna olevia tietoja, kuten myös järjestelmien välillä liikkuvia tietoja tulee suojata sopivilla hallintakeinoilla. Järjestelmien ja laitteiden käyttöä tulee suojella esimerkiksi palomuureilla, käyttäjien autentikoinnilla ja käyttöoikeuksilla. (Whitman & Mattord 2005, s. 37-38)

Näiden tietoturvallisuuden tavoitteiden saavuttamiseksi on organisaatiossa määriteltävä tietoturvallisuuden vastuut (Peltier et al. 2005; Whitman & Mattord 2005). Peltier et al. (2005) mukaan vastuita tulee jakaa organisaation johdolle, tietoturvaryhmälle, liiketoimintapäälliköille, esimiehille, työntekijöille sekä kolmannen osapuolen toimijoille.

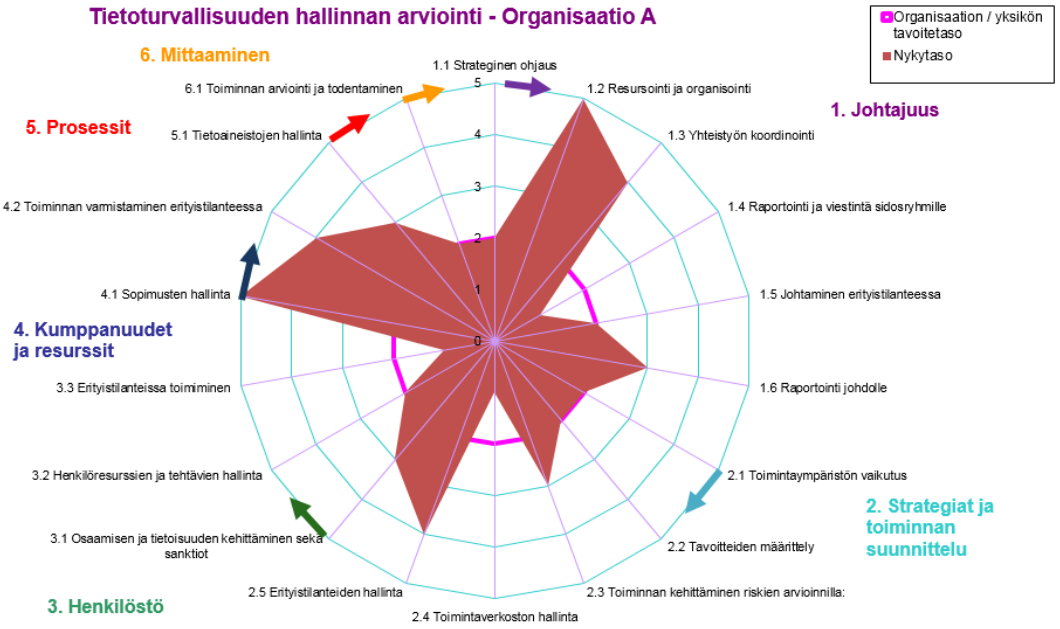
Whitman & Mattord (2005) lisäävät tähän myös tiedon omistajuuksien määrittelyn, esimerkiksi tiedon omistaja, tiedon hallussapitäjä ja tiedon käyttäjä. Erityisesti johdon sitoutuminen mahdollistaa puitteet kaiken muun tietoturvatoiminnan tekemiselle. Ilman johdon sitoutumista se ei yleensä saavuta lainsäädännöllisiä velvoitteita, eikä tue tavoiteltavia hyötyjä (Andreasson & Koivisto 2013, s. 33).

Tietoturvallisuutta voidaan tarkastella Miettisen (1999) mukaan kolmesta eri tarkastelukulmasta, liiketoiminnallisesta, prosessitason ja toteutusteknisestä tarkastelukulmasta. Liiketoiminnallinen tarkastelukulma lähtee organisaation johdon ymmärryksestä, että tietoturvallisuus on tärkeä osa organisaation toimintaa. Näkökulman perusteella tietoturvallisuuden kehittämiselle ja ylläpidolle luodaan lyhyen ja pitkän aikavälin tavoitteet, jotka liitetään osaksi organisaation päivittäistä toimintaa. Tietoturvallisuutta tarkastellaan tällöin ylhäältä alaspäin, jolloin johto pystyy määrittelemään toiminnan linjaukset, tavoitteet, politiikat sekä strategiat. Toinen tarkastelukulma on prosessitaso, joka perustuu ajatukseen, että organisaation toiminta koostuu toimintaprosesseista ja resursseista. Resurssit voivat olla joko fyysisiä tai ei-fyysisiä suojattavia kohteita. Fyysinen omaisuus on esimerkiksi organisaation laitteet ja ei-fyysinen omaisuus niissä olevat tiedot ja ihmisten taidot. Prosessitason tarkastelukulma osoittaa organisaation suojattavat kohteet prosessien ja resurssien muodossa. Kolmas tarkastelukulma tarkastelee suojausmenetelmien ylläpitäjien ja kehittäjien näkökulmaa. Toteutustekninen tarkastelukulma vastaa kysymykseen, miten organisaation tarvitsemat suojaukset toteutetaan käytännön tasolla. (Miettinen 1999) Kuva 2.2 esittää organisaation toiminnan kaikki osa-alueet huomioivan tietoturvallisuuden toimintamallin.



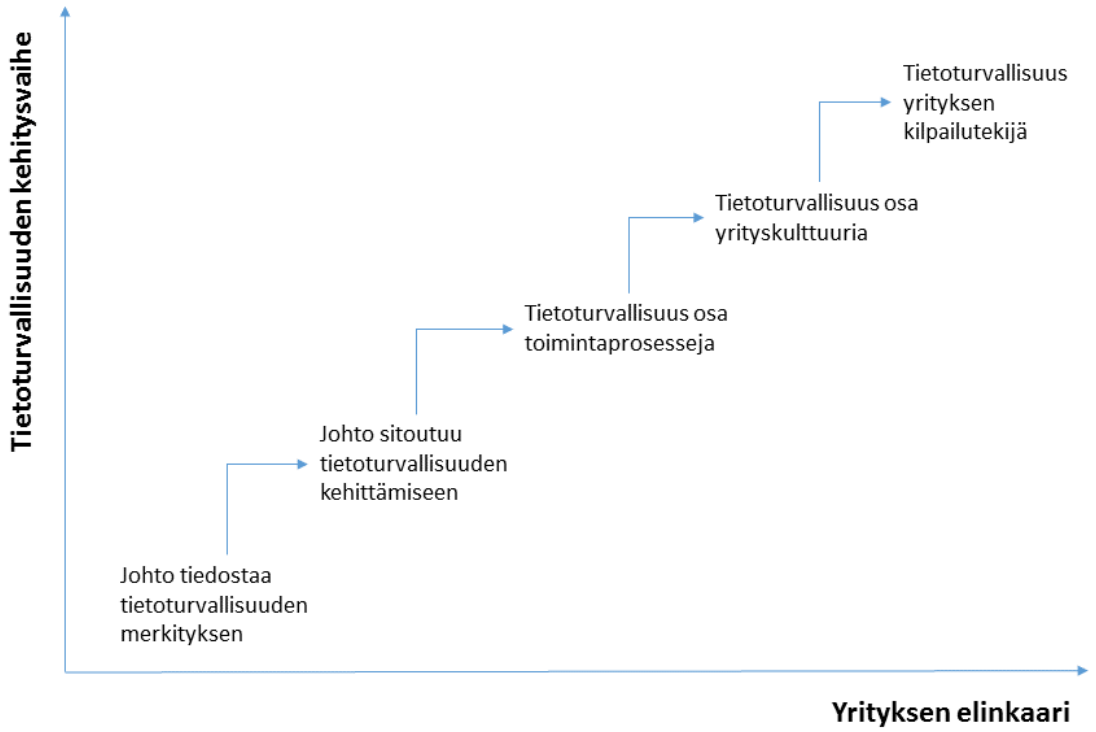
Kuva 2.2. *Tietoturvallisuuden tarkastelukulmat (Mukailtu lähteestä Miettinen 1999)*

Tietoturvan tavoitteiden saavuttamiseksi pitää ensin selvittää, mikä on tietoturvallisuuden nykyinen tila. Tietoturvallisuuden nykytila voidaan selvittää nykytila-analyysin perusteella tai organisaatio voi itse arvioida sitä VAHTI (2/2010) ohjeen mukaisella tietoturvallisuuden hallinnan arviointi taulukon avulla. VAHTI (2/2010) ohjeen yhteydestä löytyy valmis Excel-pohja, jonka täyttämällä saa muodostettua kuvan organisaation tietoturvallisuuden nykytilasta ja tavoitetasosta. Kuvassa 2.3 on esimerkki ohjeen avulla tehdystä hämähäkkikuvaajasta.



Kuva 2.3. *Tietoturvallisuuden hallinnan nykytaso ja tavoitetaso (Mukailtu lähteestä VAHTI 2/2010)*

Kuvasta 2.3 nähdään, että kyseessä olevalla organisaatiolla on tavoitetasona jokaisella osa-alueella taso 2. Kolmella alueella tämä tavoite ei toteudu, näitä alueita ovat raportointi ja viestintä sidosryhmille, toimintaverkoston hallinta ja erityistilanteissa toimiminen. Kuvan mukaisella arvioinnilla on helppoa selvittää tärkeimmät tietoturvallisuuden kehityskohteet, jotta tavoiteltu taso voidaan saavuttaa. Tehdyn arvioinnin perusteella on helpompaa perustella johdolle jonkin osa-alueen kehittämistarvetta tai liittää kuva normaalin tietoturvaraportoinnin yhteyteen selventämään tietoturvan nykytilan ja tavoitteen välistä erotusta (Andreasson & Koivisto 2013). Kun organisaation johto ymmärtää tietoturvallisuuden tärkeyden toiminnalleen, voidaan sitä lähteä kehittämään (Miettinen 1999). Wood & Saari (1992) ovat esittäneet tietoturvallisuuden kehitysvaiheet kuvan 2.4 mukaisesti.



Kuva 2.4. *Tietoturvallisuuden kehitysvaiheet (Mukailtu lähteestä Wood & Saari 1992)*

Kuvan 2.4 mukaisesti organisaation tietoturvallisuuden kehittäminen alkaa, kun johto tiedostaa tietoturvallisuuden merkityksen. Hiljalleen tietoturvallisuutta sitoudutaan kehittämään ja edelleen siitä tulee osa toimintaprosesseja ja yrityskulttuuria. Optimaalisessa tilanteessa tietoturvallisuus voi toimia organisaation kilpailuetuna. Kilpailuetu näkyy yleensä hyvänä asiakaspalveluna, laadukkaina tuotteina ja palveluina, luottamusta herättävänä yrityskuvana julkisuudessa sekä sitoutumisena tietoturvallisuuden järjestelmälliseen kehittämiseen (Miettinen 1999).

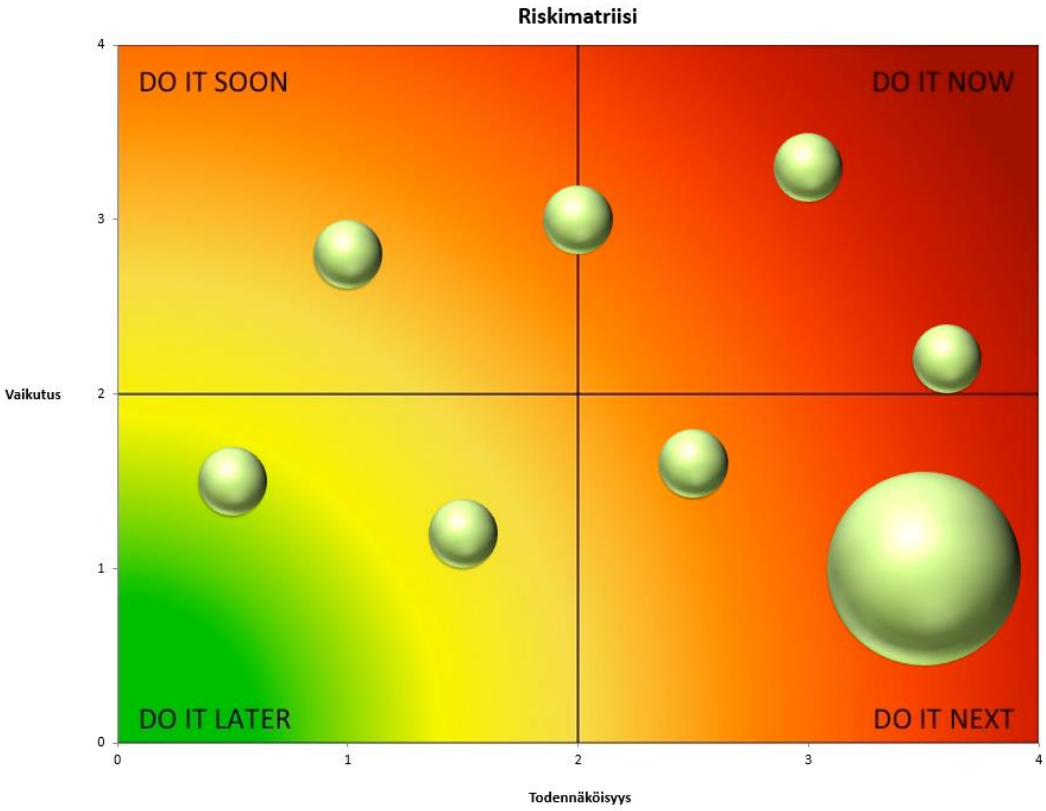
Tietoturvallisuuden huomioimisella organisaation koko toiminnassa voidaan saavuttaa monia hyötyjä liiketoiminnalle. Usein ongelmana kuitenkin on, että tietoturvallisuutta aletaan pohtia vasta, kun jotain menee pieleen. Tällöin ollaan monesti jo peruuttamattomasti ongelmissa, kun esimerkiksi asiakastietoja on vuotanut tai liiketoiminta pysähtyy palvelunestohyökkäyksen toimesta. Tietoturvallisuutta toteutetaan monesti erillisinä komponentteina, eikä sisäänrakennettuna osana organisaation toimintaa. Tietoturvan toteuttaminen on prosessi, johon tulee kuulua luonnollisena osana ajan seuraaminen ja jatkuva uudistuminen (Oksala 2013). Tällä tarkoitetaan, että tietoturvallisuutta tulisi miettiä jo ennen kuin mitään pahaa pääsee tapahtumaan, minkä lisäksi tietoturvallisuutta pitäisi ajatella organisaation prosessina. Tätä prosessia tulee kehittää, kuten muutakin organisaation liiketoimintaa, joskin ongelmana on usein resurssien puute (Andreasson & Koivisto 2013). Toinen tietoturvallisuuden toteuttamista vaikeuttava tekijä on lainsäädäntö, joka muuttuu jatkuvasti, erityisesti tietosuojaan liittyen. Lisäksi erilaiset tietojärjestelmät hankitaan usein palveluina, joiden tarkemmasta tietojenkäsittelystä ei vält-

tämättä ole suoranaisesti saatavilla tietoa. Missä organisaation tiedot järjestelmässä fyysisesti ovat, kuka tiedot omistavat ja miten palvelun lopettamisen yhteydessä tiedoille käy? Nämä ovat kysymyksiä, joita voidaan hallita suunnitelmallisen sopimustenhallinnan avulla, mutta sekään ei toimi suurien palvelutalojen yhteydessä. Tämän vuoksi organisaatioissa tehdään riskienhallintaa osana tietoturvallisuuden hallintaa.

2.4 Riskienhallinta osana tietoturvallisuutta

Kaikkeen organisaation toimintaan liittyy aina riskejä, jotka ymmärtämällä voidaan varmistaa liiketoiminnan häiriötön toiminta. Organisaation liiketoiminnan jatkuvuuden vuoksi nämä riskit tulee tunnistaa, ymmärtää ja tehdä niiden perusteella päätökset, miten niihin varaudutaan. Riskien tunnistamiseksi tulee tehdä riskianalyysi, jolla tunnistetaan organisaatioon kohdistuvat riskit. Peltier et al. (2005) muotoilevat riskianalyysin toiminnaksi, joka mahdollistaa organisaation oman kohtalon hallinnan. Tällä tarkoitetaan tehokkaan riskianalyysin perusteella tehtävää riskienhallintaa, jolla tartutaan vain oikeasti tärkeisiin ja juuri kyseessä olevaa organisaatiota koskeviin riskeihin. Whitman & Mattord (2005) pitävät riskien tunnistamista riskienhallintaprosessin ensimmäisenä osana. Toisena osana he näkevät riskien kontrolloinnin, mikä tarkoittaa riskien vähentämiseksi tehtäviä toimenpiteitä. Riskien tunnistaminen sisältää riskianalyysin, resurssien inventoinnin, resurssien luokittelu ja uhkien sekä haavoittuvuuksien tunnistaminen. Riskien kontrollointi käsittää strategian valitsemisen ja hallintatoimenpiteiden päättämisen.

Riskienhallinta voidaan nähdä Tipton & Krausen (2004) mukaan myös tasapainotteluna riskin realisoitumisen hinnan ja sen suojaamiseen käytettyjen resurssien välillä. Riskejä arvioidaan usein niiden liiketoiminnallisten vaikutusten ja esiintymisen todennäköisyyden perusteella. Näiden kahden mittarin perusteella voidaan laittaa tunnistetut riskit riskimatriisiin, jossa y-akselilla on vaikutus ja x-akselilla todennäköisyys (Miettinen 1999; Krutz & Vines 2004). Matriisista nähdään nopeasti, mitkä riskit vaativat välitöntä reagoimista, jotta riski ei pääse realisoitumaan. Tapahtuessaan riski voi aiheuttaa liiketoiminnalle negatiivisia vaikutuksia, kuten brändin alenemista, liiketoiminnan keskeytymisen tai tietojen vuotamisen organisaation ulkopuolelle. Tietoturvan kannalta riskit käsittelevät yleisesti ottaen tiedon turvallisuutta organisaatiossa. Organisaatioissa on tietoa kaikkialla, henkilöissä hiljaisena tietona, tietojärjestelmissä tallennettuna sekä prosesseissa. Alla olevassa kuvassa 2.5 on esitetty yksi mahdollinen riskimatriisi.



Kuva 2.5. *Riskimatriisi*

Matriisi voidaan myös ajatella nelikenttänä, joista jokainen osa kuvaa riskin vähentämisen tarvetta. Oikeassa yläkulmassa ovat vaikutuksiltaan kaikkein suurimmat ja suurimman todennäköisyyden riskit, joiden hallitsemiseksi tulee tehdä toimenpiteitä heti. Oikealla alhaalla on hieman pienemmän vaikutuksen riskit, jotka ovat kuitenkin erittäin todennäköisiä. Näitä riskejä tulee hallita seuraavaksi. Vasemmassa yläkulmassa olevat riskit ovat vakavia seuraamuksiltaan, mutta niiden tapahtuminen on melko epätodennäköistä. Nämä riskit tulee tunnistaa ja niiden tilaa tulee tarkkailla. Vasemmassa alakulmassa olevat riskit ovat kaikkein pienimpiä niin vaikutuksiltaan kuin todennäköisyydeltään ja nämä riskit voidaan usein hyväksy sellaisenaan, ilman erillistä hallintaa. Tipton & Krause (2004, s. 734-735) jakavat riskienhallinnan vaadittaviin ja riittäviin toimenpiteisiin. Matriisin kahdessa ensimmäiseksi esitellyssä solussa olevat riskit vaativat erillisiä toimenpiteitä riskin hallitsemiseksi ja vastaavasti kahdessa jälkimmäisessä solussa olevien riskien hallintaan riittää niin sanottu tietoturvallisuuden perustaso.

Riskin aiheuttamia liiketoiminnallisia vaikutuksia on Brotbyn (2009, s. 108) mukaan vaikeaa arvioida. Vaikutukset voivat olla joko välittömästi ja välillisesti rahallisia, mikäli liiketoiminta perustuu verkossa tapahtuvaan palveluun, on sen katkeaminen välittömästi verrattavissa rahallisiin menetyksiin. Mikäli kyseessä on esimerkiksi pankin tietojen vuotaminen, on se välillisesti liitoksissa pankin brändin arvon laskuun, mikä saattaa näkyä muun muassa osakkeen hinnassa. Toisaalta kummassakin tilanteessa on

vaikeaa arvioida rahallista arvoa riskin sattumiselle, erityisesti jos organisaatio ei ole luokitellut tietojaan ja määritellyt eri tiedoille niiden arvoja (Krutz & Vines 2004, s. 31-32). Tietojen arvoja voidaan luokitella Whitman & Mattrod (2005) mukaan esimerkiksi kategorioilla luottamuksellinen, yrityksen sisäinen ja julkinen.

Toinen riskin arviointiin käytetty tekijä on todennäköisyys, jota on myös hankalaa arvioida, sillä moni riski voi tapahtua monella eri tavalla (Brotby 2009, s. 125-136; Krutz & Vines 2004, s. 24-25). Esimerkiksi tiedon vuotaminen voi tapahtua ohjelmiston haavoittuvuuden, järjestelmävirheen tai työntekijän toiminnan kautta. Peltier et al. (2005, s. 190) sekä Ozier (2004, s. 803) suosittelevat käyttämään riskin vaikutuksen ja todennäköisyyden arvioinnin asteikkona matala, keskiverto ja korkea –asteikkoa, sillä tarkempien arvojen määrittäminen voi olla hankalaa. Todennäköisyyden kohdalla aikaväli riskin toteutumiselle on yksi vuosi. Esimerkiksi millä todennäköisyydellä organisaation järjestelmään kohdistuu palvelunestohyökkäys seuraavan vuoden aikana. Ozier (2004) näkee riskien hallinnan tarkoittavan uhkakuvien etsimistä, niiden seurausten tai vaikutusten arvioimista ja niiden toteutumisen tiheyden arviointia. Lisäksi hän korostaa edellä mainittujen arvioiden paikkansapitävyyttä, eli voidaanko arvioihin luottaa. Taulukossa 2.2 on esitetty eri lähteistä löytyneitä määritelmiä riskin ja uhan eroavaisuuksille.

***Taulukko 2.2**: Riskin ja uhan määritelmät*

Lähde	Riski	Uhka
Andreasson & Koivisto (2013)	Epävarmuuden vaikutus tavoitteisiin	
Kaplan (2004)	Tietyn tapahtuman todennäköisyys ja kustannus tapahtuessaan.	Olosuhde tai tapahtuma, joka saattaa aiheuttaa harmia järjestelmälle (Datan tuhoutuminen, paljastuminen, muuttuminen tai palvelun estyminen)
Miettinen (1999)	Riski koostuu kolmesta komponentista - Uhka - Epävarmuus - Mahdollisuus	Aiheuttaa riskin yrityksen toiminnalle
Ozier (2004)	Mahdollisuus haitan tai häviön tapahtumiselle - Mikä on uhka? - Mikä sen seuraus tai vai-	Tapahtuma, jonka tapahtumisella voi olla epätoivottuja vaikutuksia

	kutus on? - Kuinka usein se tapahtuu? Kuinka varmoja edelliset kolme vastausta ovat?	
Whitman & Mattord (2005)	Riski on todennäköisyys, että jotain voi tapahtua	Kohde, henkilö tai muu taho, joka aiheuttaa mahdollisen vaaran resurssille

Riskit sisältävät usein käsityksen uhan todennäköisyydestä ja sen vaikutuksesta liiketoimintaan, kun taas uhka nähdään tapahtumana, ilman huomioita todennäköisyydestä tai mahdollisista vaikutuksista. Uhat ovat siis osa riskin määritelmää, kuten Ozier (2004) asian ilmaisee. Tämä tutkimus käsittelee tietoturvatapahtumia uhkina, sillä kuten aiemmin todettiin, riskien vaikutuksia ja todennäköisyyttä on vaikeaa arvioida. Lisäksi tämä tutkimus ei liity mihinkään määriteltyyn tutkittavaan järjestelmään tai sovellukseen, jolloin on mahdotonta määrittää yleisesti päteviä vaikutuksia ja todennäköisyyksiä uhille.

Uhkien hallintakeinot voidaan jakaa estäviin, havaitseviin ja suojaaviin (Krutz & Vines 2004). Miettinen (1999, s. 144-145) jakaa hallintakeinot ennalta estäviin, havaitseviin ja korjaaviin suojauskeinoihin. Kaikki hallintakeinot eivät kuulu vain johonkin edellä mainituista ryhmistä, jotkin hallintakeinot saattavat kuulua näistä jopa jokaiseen. Tässä tutkimuksessa tietoturvallisuuden hallintakeinoja on jaoteltu Krutz & Vines (2004) esittelemän jaon mukaisesti. Sharp (2004, s. 768-770) on määritellyt riskienhallinnan ensisijaisiksi toiminnoiksi:

- Autentikoinnin
- Pääsynhallinnan
- Yksityisyyden
- Datan eheyden
- Kiistämättömyyden

Riskienhallintaa voidaan suorittaa tietoturvallisuuden hallintajärjestelmän mukaisesti vaiheittain PCDA-mallin avulla (Andreasson & Koivisto 2013, s. 42-43). PCDA-malli koostuu neljästä osasta, suunnittelusta (plan), toteutuksesta (do), arvioinnista (check) ja toimimisesta (act). Mallia on viety pidemmälle ja sovitettu toimimaan paremmin riskienhallinnan yhteydessä muun muassa Peltier et al. (2005) ja Miettinen (1999) toimesta. Peltier et al. (2005, s. 187-191) määrittelee prosessin osa-alueet seuraavasti:

- Resurssien määrittely
- Uhkien tunnistaminen

- Tapahtumien todennäköisyyden arviointi
- Vaikutusten arviointi
- Tarvittavien hallintatoimenpiteiden määrittely
- Dokumentointi

Miettinen (1999, s. 95-98) määrittelee laajennetun PCDA-malliin perustuvan tietoturvallisuuden johtamisen mallin, jota voidaan soveltaa myös riskienhallintaan seuraavasti:

- Riskien tunnistaminen
- Suojaustason määrittely
- Suojausten suunnittelu
- Suojausten toteutus
- Suojaustason valvonta
- Suojausten kehittäminen

Kaikkia uhkia ei voida koskaan hallita, eikä kaikilta uhilta suojautua. Kaikilta uhilta suojautuminen ei ole kustannustehokasta, eikä yleisesti ottaen myöskään mahdollista johtuen rajallisista resursseista. Tämän vuoksi riskienhallinnan yhteydessä puhutaan usein päätöksistä, jotka määrittelevät mitä uhan suhteen tehdään. Uhkien hallitsemisen toteutuskeinoja ovat uhan poistaminen, vähentäminen, siirtäminen, ulkoistaminen ja hyväksyminen (Henry 2004, s. 757-758; Miettinen 1999, s.56-57; VAHTI 7/2003; Whitman & Mattord 2005, s. 138-144). Nämä hallinnan toteutuskeinot sisältävät käytännössä lähes kaikki yksittäiset konkreettiset tavat hallita uhkia. Uhan poistaminen tähtää siihen, että uhka saadaan kokonaan poistettua. Usein uhan poistaminen ei ole mahdollista tai vaatisi huomattavan suuria resursseja (Miettinen 1999, s. 56). Uhan vähentämisen tavoitteena on pienentää uhan mahdollisia vaikutuksia ja siihen sisältyy usein organisaation toiminnan jatkuvuussuunnittelua uhan toteutumisen varalta (Whitman & Mattord 2005, s. 142-144). Uhan siirtäminen on käytännössä uhan vaikutusten tietoista siirtämistä toisen osapuolen vastuulle, mikä yleisesti ottaen tarkoittaa tietyn asian vakuuttamista tai palvelutasosopimusta. Uhan ulkoistaminen on yleistynyt, kun markkinoille on tullut entistä enemmän yrityksiä, jotka huolehtivat toisen yrityksen tietoturvasta palveluna. Tässä tapauksessa kolmas osapuoli on sopimuksen mukaisesti vastuussa uhkien toteutumisesta aiheutuvista vaikutuksista (Henry 2004, s. 757). Viimeisenä mahdollisuutena on hyväksyä uhka sellaisenaan, mikäli sen mahdollisesti aiheuttamat vaikutukset ovat pienet, mahdollisuus hallita sitä on pieni tai sen hallinta ei ole kustannustehokasta (Henry 2004, s. 758; Miettinen 1999, s. 57).

2.5 Tietoturvallisuuden uhkien kategorisointi

Tietoturvallisuuden uhkia voidaan kategorisoida monella tavalla ja kategorioiden sisälle kerätä konkreettisia uhkia niiden soveltuvuuden mukaan. Peltier et al. (2005, s. 21-38) esittelee kategorioiksi virheet ja laiminlyönti, petokset ja varkaudet, pahansuovat hakkerit, pahansuovan koodin, palvelunestohyökkäykset ja sosiaalisen manipuloinnin. Whit-

man (2003) on tunnistanut 12 tietoturvallisuuden uhkaa, jotka ovat hänen tekemänsä kyselyn mukaan painotetussa tärkeysjärjestyksessä (suluissa painoarvo):

- Harkitut sovellushyökkäykset (2178)
- Ohjelmistovirheet (1130)
- Inhimilliset virheet ja erehdykset (1101)
- Harkittu vakoilu tai tunkeutuminen (1044)
- Harkittu sabotointi tai vandalismi (963)
- Teknisen laitteiston virheet ja hajoaminen (942)
- Harkitut varkaudet (695)
- Luonnonilmiöt (611)
- Immateriaalisten resurssien vaarantuminen (495)
- Poikkeamat palvelun laadussa (434)
- Vanhentuneet teknologiat (428)
- Harkittu tiedon kiristäminen (225)

Listan ensimmäisenä, eli suurimman painoarvon kategoriana ovat harkitut sovellushyökkäykset, joiden painoarvo on lähes kaksinkertainen toisena olevaan ohjelmistovirheiden kategoriaan. Muut kategoriat ovat selkeästi tasaisemmin painottuneita toisiinsa verrattuna. Toiseksi painottunut ohjelmistovirheet, voidaan nähdä sekä uhkana että haavoittuvuutena. Haavoittuvuus on tässä tapauksessa uhan mahdollistaja. Ohjelmistovirheet nähdään suorana uhkana tiedolle, kun ohjelmiston toiminta aiheuttaa tiedon muuttumista ja vaarantaa näin ollen eheyden tai yksinkertaisesti estää tiedon saatavuuden. (Whitman 2003)

Whitman & Mattord (2005, s. 38-68) ovat avanneet tätä Whitman (2003) tekemää listausta varsin laajasti. Listaus sisältää suurimman osan Peltier et al. (2005) määrittelemistä kategorioista hieman laajennettuna. Peltier et al. (2005) esittelemät palvelunestohyökkäykset ja sosiaalinen manipulointi kategoriat eivät ole Whitmanin (2003) listauksessa, mutta ne voidaan ymmärtää toisten kategorioiden osaksi. Palvelunestohyökkäykset voidaan katsoa kuuluvan harkittuihin sovellushyökkäyksiin ja sosiaalinen manipulointi osaksi inhimillisiä virheitä ja erehdyksiä.

Miettinen (1999, s. 34-37) on käsitellyt tietoturvallisuuden uhkia vielä hieman yleisemmällä tasolla, saaden kategorioiksi vahingossa syntyneet ja tarkoituksella aiheutetut, passiiviset ja aktiiviset, sisäiset ja ulkoiset sekä ihmisen aiheuttamat ja luonnosta johtuvat uhat. Hän on jaotellut erikseen tietojenkäsittelyn uhat tietojen tai tietojenkäsittelyresurssien tuhoutumiseen, tietojen sisällön luvattomaan muuttamiseen, tietoihin tai tietojenkäsittelyresursseihin kohdistuviin varkauksiin, katoamisiin tai muihin menetyksiin, tietojen sisällön paljastumiseen sekä tietojenkäsittelytoiminnan keskeytymiseen (Miettinen 1999, s. 37-39).

3. ESINEIDEN INTERNETIN TIETOTURVA (INTERNET OF THINGS)

Tässä luvussa tutustutaan ensimmäisenä esineiden internetin käsitteeseen ja arkkitehtuuriin. Seuraavaksi syvennytään erilaisiin sovellusalueisiin ja haasteisiin. Lopuksi tarkastellaan esineiden internetin tietoturvallisuutta sekä siihen liittyviä uhkia ja hallintakeinoja.

3.1 Esineiden internetin määritelmä

Esineiden internet on yksi tämän hetken kuumimmista trendeistä teknologia-alalla, Cearley (2016) listaa sen myös kymmenen kuumimman teknologia trendin joukkoon Forbesin vuoden 2016 listauksessa. Manyika et al. (2015) arvioi esineiden internetistä saatavan ekonomisen vaikutuksen olevan neljästä yhteentoista triljoonaa dollaria vuositasolla, vuoteen 2025 mennessä. Suurin mahdollinen vaikutus arvioidaan olevan teollisuudelle, missä vaikutukset voivat olla jopa 3,7 triljoonaa dollaria vuodessa. Arvion yläpää vastaisi toteutuessaan noin yhtätoista prosenttia maailmantaloudesta. Potentiaalia esineiden internetin mahdollisuuksista ei puutu, mutta saavuttaakseen edellä mainitut arvioit, tulee selvittää tekniset, organisationaaliset ja vaatimukselliset haasteet (Manyika et al. 2015).

Esineiden internet ei kuitenkaan ole aivan uusia asia, sillä Kevin Ashton esitteli käsitteen Internet of Things jo vuonna 1999, työskennellessään yrityksessä Procter & Gamble (Ashton 2009). Esineiden internetistä käytetään edelleen monia eri nimityksiä ja monet niistä ovat päällekkäisiä, mikä vaikeuttaa tutkimusta (Haller 2010). Ilmiön ympärille on muodostunut varsin monimuotoinen käytäntö eri termeistä ja niiden käytöstä ja merkityksestä (Atzori et al. 2010). Ilmiöstä puhutaan nimillä esineiden internet, asioiden internet ja teollinen internet. Suomenkielisten termien lisäksi käytetään myös englanninkielisiä termejä, kuten Internet of Things (IoT), Machine-to-Machine (M2M), Internet of Everything (IoE) ja Industrial Internet (of Things) sekä näiden vapaita yhdistelmiä.

Ilmiön ja käytettävien termien välisten erojen ymmärtämiseksi tulee perehtyä termien määritelmiin tarkemmin. Seuraavassa on esitelty taulukoituna määritelmiä termeille Internet of Things, M2M sekä Industrial Internet. Tässä tutkimuksessa käytetään suomenkielistä termiä esineiden internet, joka on määritelmistä lähimpänä englanninkielistä termiä Internet of Things. Termi esineiden internet kuvaa parhaiten työssä valittua aihetta ja tutkimuksen apuna käytettyjä esimerkkejä.

Taulukko 3.1. *Kirjallisuuden määritelmiä termille Internet of Things (IoT)*

Internet of Things	
Bassi et al. 2008	**Funktionaalinen näkökulma:** Asiat, joilla on identiteetit ja virtuaaliset persoonallisuudet, toimivat älykkäissä tiloissa käyttäen älykkäitä rajapintoja yhteyksien luomiseen sekä kommunikointiin sosiaalisessa, ympäristöllisessä ja käyttäjälähtöisessä kontekstissa. **Saumattoman integraation näkökulma:** Toisiinsa kytketyt objektit, joilla on aktiivinen rooli niin kutsutussa tulevaisuuden internetissä. **Semanttinen näkökulma:** Maailmanlaajuinen, standardoituihin viestintäprotokolliin perustuva verkosto, toisiinsa kytkettyjä objekteja, jotka ovat yksilöllisesti tunnistettavia.
Chen 2012	Älykkäät laitteet keräävät dataa, välittävät informaatiota toisillensa, prosessoivat tietoa yhteistyössä ja suorittavat automaattisia toimenpiteitä. IoT tunnetaan myös nimellä M2M.
Chui et al. 2010	Fyysisiin objekteihin sulautetut sensorit ja toimijat ovat linkitettyinä langallisiin ja langattomiin verkkoihin, jotka käyttävät usein samaa internet protokollaa (IP), joka yhdistää internetin.
Foster 2015	Maailma, jossa fyysiset objektit ovat saumattomasti integroitu tietoverkostoon ja missä fyysisistä objekteista voi tulla aktiivisia osallistujia liiketoimintaprosesseihin.
GSMA 2014	IoT kuvaa useiden verkostojen kautta internettiin liittyneiden laitteiden ja koneiden koordinointia. Laitteet voivat olla tabletteja, kuluttajaelektroniikkaa, tai muita koneita, kuten kulkuneuvoja, monitoreja tai sensoreita, joissa on M2M viestintäyhteydet datan lähettämiseksi ja vastaanottamiseksi.
Haller et al. 2008	Maailma, jossa fyysiset objektit on integroitu saumattomasti tietoverkkoon ja jossa ne voivat osallistua aktiivisesti liiketoimintaprosesseihin. Internetissä saatavilla olevat palvelut voivat olla vuorovaikutuksessa älykkäiden objektien kanssa ja kysyä niiden tilaa sekä kaikkia niihin liittyviä tietoja, huomioimalla kuitenkin tietoturvallisuuden sekä yksityisyyden.
ISO/IEC 2014	Yhdistettyjen asioiden, ihmisten, järjestelmien ja tietoresurssien infrastruktuuri, yhdessä älykkäiden palveluiden kanssa, mikä mahdollistaa sekä fyysisen että virtuaalisen maailman tiedon prosessoinnin ja siihen reagoimisen.

ITU-T 2012	Tietoyhteiskunnan globaali infrastruktuuri, joka mahdollistaa kehittyneet palvelut, yhdistämällä fyysiset ja virtuaaliset ’asiat’, perustuen olemassa oleviin ja kehittyviin yhteentoimiviiin informaatio- ja kommunikaatio teknologioihin. IoT hyödyntää ’asioita’ kokonaisvaltaisesti, tarjotakseen palveluita kaikenlaisille sovelluksille, käyttäen hyödyksi tunnistamista, datan keräämistä, prosessointia ja kommunikaatio kyvykkyyksiä, säilyttäen vaadittavan yksityisyyden.
Reddy 2014	Älykäs verkko, joka koostuu toisiinsa liitetyistä ja yksilölliset identiteetit omaavista objekteista. Objekteilla on ominaisuus aistia, vuorovaikuttaa ja kommunikoida toistensa kanssa, niiden tilasta ja ympäristöstä käyttäen sulautettuja kommunikointi ja prosessointi teknologioita.
Vermesan et al. 2011	Dynaaminen globaali verkkoinfrastruktuuri, jolla on oma konfigurointikyky ja joka perustuu standardoituihin ja yhteensopiviin viestintäprotokolliin. Fyysisillä ja virtuaalisilla ’asioilla’ on identiteetit, fyysisiä ominaisuuksia ja virtuaaliset henkilöllisyydet ja ne käyttävät älykkäitä rajapintoja osana saumattomasti integroitua tietoverkkoa.

Esineiden internetin määritelmiä löytyisi paljon lisääkin, mutta tähän on taulukoitu muutamia niistä. Taulukossa 3.1 esiteltyjä määritelmiä analysoimalla havaitaan, että termin määritelmissä on ristikkäisyyttä ja epämääräisyyttä. Tämä johtuu osittain siitä, että asiaa on tutkittu hieman eri näkökulmista. Ilmiötä voidaan tutkia asioiden (things) ja internetin näkökulmasta, minkä lisäksi Bassi et al. (2008) lähestyvät sitä semanttisesta näkökulmasta. Toisaalta määritelmien ristikkäisyys johtuu siitä, että esineiden internet koostuu internetin ja fyysisten asioiden yhdistämisestä, jotka ovat hyvin erilaisia komponentteja.

Fyysisen ja virtuaalisen maailman yhdistäminen korostui määritelmissä, minkä lisäksi määritelmät sisältävät yleisesti asiaa älystä, integroitumisesta, globaaliudesta, infrastruktuurista sekä kokonaan omasta maailmasta. Standardointiin erikoistuvien yhdistysten (ISO, ITU) määritelmät olivat kaikkein kattavimpia, minkä vuoksi niitä voidaan pitää myös tämän tutkimuksen määritelmänä esineiden internetille. ITU-T (2012) määritelmän mukaan esineiden internet hyödyntää asioiden tunnistamista, datan keräämistä, sen prosessointia ja eteenpäin kommunikointia. Määritelmässä otetaan ainoana huomioon yksityisyys, mikä liittyy läheisesti tietoturvallisuuteen.

Yksinkertaistettuna esineiden internet koostuu datan keräämisestä, sen kommunikoimisesta eteenpäin toiselle laitteelle, mikä mahdollistaa erilaisten sovellusten toiminnan. Fyysiset laitteet, kuten ajoneuvo tai älykello, liitetään osaksi esineiden internetin järjestelmää liittämällä ne internetiin. Näin saadaan fyysinen ja virtuaalinen maailma yhdistettyä, minkä ympärille voidaan rakentaa laajempi infrastruktuuri, jossa laitteet toimivat

lähes autonomisesti, lähettäen ja vastaanottaen dataa. Optimitilanteessa laitteet voivat tehdä myös päätöksiä datan perusteella, esimerkiksi tehtaassa tapahtuvan prosessin painetta mittaava sensori huomaa nousseen paineen, minkä perusteella voidaan muuttaa prosessin asetuksia paineen tasaamiseksi normaaliin arvoon, ilman ihmisen osallistumista.

M2M eroaa esineiden internetistä määritelmien mukaan olemalla esineiden internetin mahdollistava tekijä. GSMA:n (2014) määritelmän mukaan M2M on olennainen osa esineiden internetiä, joka kuvaa sovelluksia, jotka mahdollistavat laitteiden välisen viestinnän. Watson et al. (2004) luonnehtivat termin M2M viittaavan teknologioihin, jotka mahdollistavat esineiden internetin kaltaisen toiminnan. Myös Ericsson (2014) viittaa termillä ratkaisuihin, jotka mahdollistavat viestinnän sensoreiden, hyödykkeiden ja tietojärjestelmien välillä. Ainoa hieman eroava määritelmä ottaa myös huomioon, että tiedonsiirtoon ei tarvita ihmisen osallistumista ja että sen tavoitteena on parantaa tehokkuutta ja laatua (Gupta & Hirdesh 2007).

Taulukko 3.2. *Kirjallisuuden määritelmiä termille M2M*

M2M	
Ericsson 2014	M2M viittaa ratkaisuihin, jotka mahdollistavat viestinnän sensoreiden (jotka mittaavat esim. lämpötilaa, painetta, kosteutta), hyödykkeiden (esim. autot, älykkäät mittarit) ja tietojärjestelmien välillä.
GSMA 2014	M2M on olennainen osa Internet of Thingsiä, joka kuvaa sovelluksia, joiden toiminnan mahdollistaa kahden tai useamman laitteen välinen viestintä.
Gupta & Hirdesh 2007	M2M viittaa laitteiden väliseen tiedonsiirtoon ilman ihmisen osallistumista. M2M voi tarkoittaa myös sensoreiden, toimijoiden, väliohjelmistojen, ohjelmistojen ja sovellusten muodostamaa joukkoa, joka auttaa parantamaan tehokkuutta ja laatua, sitomalla ne liiketoimintaprosesseihin.
Watson et al. 2004	M2M viittaa teknologioihin, jotka mahdollistavat tietokoneiden, sulautettujen prosessorien, älykkäiden sensorien, käyttölaitteiden ja mobiililaitteiden kommunikaation toistensa kanssa, päätöksenteon sekä toiminnan usein ilman ihmisen osallistumista.

Termi Industrial Internet viittaa useimmiten nimensä mukaisesti valmistavaan teollisuuteen. Termin suora suomennos teollinen internet on laajassa käytössä, mutta sillä viitataan usein enemmän termin Internet Of Things määritelmiin, kuin Industrial Internet termin määritelmiin. Industrial Internetin määritelmät ovat lähellä Internet Of Thingsin

määritelmiä, mutta sisältävät ajatuksen tehdasympäristöstä. Foster (2015) luonnehtii Industrial Internetiä teollisten laitteiden sensoreiden ja käyttölaitteiden yhdistymiseksi internetiin ja verkon laajentamisesta muihin tärkeisiin teollisiin verkostoihin. Vastaavasti Brunerin (2013) mukaan koneet lähettävät dataa ennalta hyväksytyille vastaanottajille ja vastaanottavat toiminnallisia käskyjä oikeutetuilta lähettäjiltä.

Taulukko 3.3. *Kirjallisuuden määritelmiä termille Industrial Internet*

Industrial Internet	
Bruner 2013	Koneista tulee solmuja (node) kokonaisvaltaisissa verkoissa, jotka käyttävät avoimia protokollia. Koneet julkaisevat dataa oikeutetuille vastaanottajille ja vastaanottavat toiminnallisia käskyjä oikeutetuilta lähettäjiltä.
Foster 2015	Industrial Internet koostuu teollisten laitteiden sensoreiden ja käyttölaitteiden yhteydestä paikalliseen prosessointiin ja internetiin sekä yhteyden laajentamisesta muihin tärkeisiin teollisiin verkostoihin, jotka voivat itsenäisesti luoda arvoa.

3.2 Esineiden internetin kolmen tason arkkitehtuuri

Esineiden internetin arkkitehtuurille on olemassa monia erilaisia malleja. Tässä tutkimuksessa käytetään Wu et al. (2010) esittelemää kolmen tason mallia, joka koostuu havainnointitasosta, siirtotasosta sekä sovellustasosta. Tutkimuksessa havainnollistetaan esineiden internetin uhkia jaottelemalla niitä näiden esineiden internetin tasojen mukaisesti. Wu et al. (2010) esittelemä esineiden internetin arkkitehtuuri ei kuitenkaan ole ainoa näkemys, joka kirjallisuudesta löytyy.

Xu et al. (2014) esittelivät esineiden internetille nelitasoisen arkkitehtuurin, joka koostuu aistimis-, tietoverkko-, palvelu- ja käyttöliittymätasosta. Tästä hieman poikkeavan, viiden tason arkkitehtuurin esittelivät Khan et al. (2012). Heidän mallinsa koostuu havainnointi-, tietoverkko-, väliohjelmisto-, sovellus- ja liiketoimintatasosta. Tan & Wang (2010) sekä Bandyopadhyay & Sen (2011) jakavat arkkitehtuurin viiteen osaan, jotka ovat reunateknologia, pääsyportti, internet, väliohjelmisto ja sovellus. Näitä kaikkia kirjallisuudessa esiteltyjä malleja arkkitehtuurille yhdistää sama esineiden internetin idea, missä alimmalla tasolla havaitaan tai aistitaan tietoa, josta muodostuu dataa. Seuraavalla tasolla dataa siirretään, yleisesti jollain internetin standardoidulla verkkoprotokollalla. Data tallennetaan tietojärjestelmään käyttäen apuna väliohjelmistoja, jotka tallentavat datan käsiteltävään muotoon, jota on jatkossa mahdollista käyttää. Ylimmällä

tasolla ovat sovellukset ja liiketoiminta, jotka hyödyntävät tallennettua tietoa tarpeen mukaan, erilaisissa tilanteissa.

Ensimmäisenä esitelty kolmen tason malli on käytännössä samaa asiaa sisältävä arkkitehtuuri kuin muutkin esitellyt mallit, sitä on vain hieman yksinkertaistettu ilmiön ymmärtämisen helpottamiseksi (Wu et al. 2010). Kolmen tason mallissa siirtotaso käsittää sisäänsä Khan et al. (2012) esittelemistä tasoista tietoverkko- sekä väliohjelmisotason. Vastaavasti ylimmällä tasolla Wu et al. (2010) sovellustaso sisältää ajatuksen Khan et al. (2012) sovellus- sekä liiketoimintatasosta. Yhtäläisesti myös muissa esitellyissä malleissa tasot voidaan katsoa sisältävän muiden arkkitehtuurien yhden tai useamman tason, riippumatta tason nimityksestä. Xu et al. (2014) esittelemät tasojen nimet eroavat hieman muista, mutta sisällöltään ne ovat rinnastettavissa muihin arkkitehtuureihin. Esineiden internetin käsitteen vakiintumattomuus ulottuu myös arkkitehtuuriin, aiheuttaen epäselvyyttä, ristiriitoja ja päällekkäisyyksiä riippuen ilmiötä tutkivasta henkilöstä ja hänen/heidän taustastaan (Krco & Carrez 2014). Seuraavaksi esitellään hieman tarkemmin kuvassa 3.1 mallinnettu, tutkimuksessa käytetty Wu et al. (2010) esittelemä kolmen tason arkkitehtuuri.

Kuva 3.1. *Esineiden internetin arkkitehtuuri (mukailtu lähteestä Wu et al. 2010)*

Havainnointitaso on esineiden internetin arkkitehtuurin hierarkian alin taso, mistä kaikki kerättävä data saadaan. Wu et al. (2010) vertaa tasoa ihmisen aisteihin, sillä aisteilla ihminen kerää dataa ympäristöstään, jota aivot lopulta hyödyntävät päätöksenteossa. Tason päätehtävänä on heidän mielestään kerätä dataa ympäristöstä ja tunnistaa kohde,

jonne data lähetetään. Havainnointitaso sisältää fyysisesti viivakoodeja, viivakoodinlukijoita, RFID-tarroja, -lukijoita, kameroita, GPS paikantimia, ympäristöä (paine, lämpötila, jne) mittaavia sensoreita ja näiden muodostaman sensoriverkoston. Riippuen sensorista tasolla voidaan kerätä dataa lokaatiosta, lämpötilasta, liikkumisesta, tärinästä, kiihdytyksestä, kosteudesta, kemiallisista muutoksista ilmassa ja niin edelleen (Khan et al. 2012).

Siirtotasolla kerätty data lähetetään sensorilta eteenpäin, kuten ihmisen hermoverkostossa viesti aivoilta lihaksille (Gang et al. 2011; Wu et al. 2010). Tasolla data lähetetään turvallisesti tietoa prosessoivaan järjestelmään käyttäen tiedonsiirtoon langallista tai langatonta verkkoa. Tiedonsiirtotapana on useimmiten jokin tunnetuista standardeista, kuten 3G, 4G, Wifi, Bluetooth tai infrapuna. (Khan et al. 2012) Siirtotaso koostuu kommunikointiverkostosta, joka on yhteydessä internetiin ja joka käyttää älykästä tiedon prosessointia, tiedon siirtämiseksi haluttuun paikkaan, halutussa muodossa (Wu et al. 2010). Tason päätehtävänä on lähettää ja prosessoida havainnointitasolta kerättyä dataa.

Sovellustaso on tutkimuksessa käytetyn arkkitehtuurin korkein taso hierarkkisesti. Sovellustason sisältö vaihtelee tarpeen mukaan toimialasta riippuen (Wu et al. 2010). Taso on yhdistelmä esineiden internetin sosiaalista verkostoa ja toimialan tarpeita, jotta laajaa älyllistämistä voidaan hyödyntää (Wu et al. 2010). Taso tarjoaa erilaisia sovelluksia erilaisille käyttäjille tiedon käsittelyyn ja päätöksenteon tueksi (Bandyopadhyay & Sen 2011). Sovellukset voivat olla erilaisilta toimialoilta, kuten valmistus, logistiikka, vähittäiskauppa, yleinen turvallisuus, terveydenhuolto, älykäs koti tai älykäs liikenne (Bandyopadhyay & Sen 2011; Khan et al. 2012). Wu et al. (2010) vertaa sovellustasoa ihmisten sosiaaliseen verkostoon, joka muodostaa lopulta koko yhteiskunnan.

Wu et al. (2010) esittelivät myös uuden viiden tason mallin esineiden internetille, joka koostuu havainnointi-, siirto-, prosessointi-, sovellus- sekä liiketoimintatasoista. Uudessa mallissa on siis kaksi uutta tasoa, prosessointitaso sekä liiketoimintataso. Tässä tutkimuksessa käytetään kuitenkin vanhaa kolmen tason mallia sen yksinkertaisuuden vuoksi.

3.3 Esineiden internetin sovellusalueet ja haasteet

Esineiden internetillä on monia sovellusalueita, mikä tekee ilmiön ymmärtämisestä monimutkaista, sillä sovellusalueesta riippuen esineiden internetin sovellukset ja toiminta ovat erilaisia. Reddy (2014) on esitellyt esineiden internetin sovellusalueiksi seuraavat

- Auto ja kuljetusala
- Terveydenhoito
- Valmistava teollisuus
- Vähittäiskauppa

- Toimitusketju
- Infrastruktuuri
- Öljy ja kaasu
- Vakuutukset
- Hyödykkeet (mittarit, verkot)

Bandyopadhyay & Sen (2011) esittelevät esineiden internetin sovellusalueiksi hieman laajennetun listauksen

- Avaruus ja lentoteollisuus
- Autoteollisuus
- Teleoperaattorit
- Terveydenhoito
- Itsenäinen asuminen
- Lääketeollisuus
- Vähittäiskauppa, logistiikka ja toimitusketjunhallinta
- Valmistava teollisuus
- Prosessiteollisuus
- Ympäristönvalvonta
- Kuljetusala
- Maatalous
- Media ja viihdeteollisuus
- Vakuutukset
- Kierrätys

Näiden kahden listauksen perusteella jo voidaan sanoa, että esineiden internet on hyvin laaja käsite, joka koskettaa lähes kaikkia aloja. Jokaisella sovellusalueella on kuitenkin erilaiset vaatimukset ja erilaiset uhat koskien tietoturvallisuutta. Terveydenhoidon eräs sovellus on sydämentahdistin, joka hälyttää automaattisesti ensiapua, mikäli henkilöllä esiintyy poikkeamia sydämenlyönneissä. Tällaisen laitteen tietoturvaa uhkaa hyvin erilaiset ongelmat, kuin esimerkiksi valmistavan teollisuuden yhteydessä tehtaassa olevaa lämpötilasensoria. Atzori et al. (2010) ovat esitelleet sovellusalueiksi typistetyn listauksen, joka koostuu neljästä toimialasta, jotka ovat kuljetus ja logistiikka, terveydenhuolto, älykäs ympäristö (koti, toimisto, tehdas) sekä henkilökohtainen ja sosiaalinen toimiala. Listauksia löytyy kirjallisuudesta mittava määrä, ja sovellusalueet riippuvat paljon kirjoittajan näkökulmasta ja omasta esineiden internetin käsityksestä. Tässä tutkimuksessa sovellusalueet eivät ole suuressa osassa, minkä vuoksi niitä ei esitellä tämän enempää. Sovellusalueiden esittelyn tarkoituksena on antaa lukijalle käsitys esineiden internetin valtavasta laajuudesta ja selittää sen monimuotoisuutta antamalla käsitys sen ulottuvuudesta eri toimialoille. Tutkimus ei rajaudu tiettyyn sovellusalueeseen, mutta haastatteluissa käytetyn esimerkin voidaan katsoa liittyvän autoteollisuuden osa-alueeseen. Tutkimuksessa käsitellään esineiden internetin tietoturvallisuutta yleisellä

tasolla, jolloin sen voidaan katsoa pätevän kaikkiin sovellusalueisiin, olematta kuitenkaan minkään alueen täydellinen kuvaus.

Babar et al. (2010) on esitellyt esineiden internetin tehtäviä, joita toimivan järjestelmän tulisi tukea mahdollisimman hyvin. Tehtäviä ovat nimeäminen ja osoitteet, laitteiden ja verkon löytäminen, sisällön ja palveluiden käyttö, kommunikaatio ja turvallisuus ja yksityisyys. Nimeäminen ja osoitteet viittaavat järjestelmään liittyneiden laitteiden yksilöintiä, kun järjestelmässä saattaa olla yhdistettynä tuhansia laitteita. Laitteiden ja verkon löytäminen on seuraava askel, sillä laitteiden tulee olla löydettävissä, jotta ne voidaan liittää osaksi verkostoa. Sisällön tulee olla eheää ja järjestelmässä tulee olla datan korruptoimisien estäviä mekanismeja. Erityisesti palveluiden, jotka sisältävät laitteiden kalibrointiin liittyvää dataa, tulisi sisältää mekanismin, jolla voidaan tunnistaa vääränlaiset syötteet järjestelmään. Laitteiden tulisi kyetä toimiaan itsenäisesti osana suurempaa verkostoa ja sietämään vikatilanteita, kuten hetkellistä katkosta internet yhteydessä. Langattoman järjestelmän turvallisuuteen ja yksityisyyteen tulee myös kiinnittää huomiota. Babar et al. (2010) huomauttavat erityisesti laitteiden nimeämiseen ja osoitteisiin kohdistuvista ongelmista, jotta jokainen verkoston laite voidaan varmentaa aidoksi ja osoittaa oikeaksi osaksi järjestelmää. Yksi uusi mahdollisuus tämän varmistamiseksi on paikannustiedon käyttäminen, sillä verkon tarjoaman tiedon tulisi olla luotettavaa.

Esineiden internetiin liittyy monenlaisia haasteita, joista tässä esitellään tietoturvallisuuteen liittyviä. Tietoturvallisuus määriteltiin aiemmin koostumaan kolmesta kivijalasta, jotka ovat luottamuksellisuus, eheys ja saatavuus. Khan et al. (2012) sekä Bandyopadhyay & Sen (2011) nostavat luottamuksellisuuden haasteeksi esineiden internetissä. Esineiden internetin laitteet keräävät ja lähettävät dataa edelleen, jolloin niiden pitää varmistua, että data lähetetään oikeille vastaanottajille (Khan et al. 2012). Bandyopadhyay & Sen (2011) sanovat luottamuksellisuuden nojaavan standardoitujen salausteknologioiden varaan, missä ongelmana on algoritmien käytön nopeus ja energiankäyttö. Esineiden internetin sovelluksissa käytön tulee olla nopeaa, mikä vaikeuttaa monimutkaisempien algoritmien käyttöä johtuen pienestä prosessointi kapasiteetista. Eheyden haasteena on, kun esineiden internetin laitteet eivät ole jatkuvassa yhteydessä verkkoon, vaan vain kun ne päivittävät tietoa. Tietoa saatetaan päästä muuttamaan, silloin kun se on vain tallennettuna laitteeseen tai kun tietoa siirretään verkossa (Atzori et al. 2010). Saatavuus puolestaan on haaste, sillä fyysisiin laitteisiin saatetaan päästä käsiksi, jolloin niitä voidaan fyysisesti vahingoittaa tai muuttaa niiden toimintaa, mikä edelleen vaikuttaa eheyteen ja luottamuksellisuuteen (Babar et al. 2010; Jing et al. 2014; Khan et al. 2012).

Standardoinnin puute on eräs haaste, joka nousee usein esille puhuttaessa esineiden internetistä. Standardeja tarvitaan kaksisuuntaiseen kommunikaatioon ja laitteiden informaation vaihtoon (Bandyopadhyay & Sen 2011). Tällä hetkellä esineiden internet koostuu todella laajasta kirjosta erilaisia laitteita, jotka toimivat erilaisilla teknologioilla (Babar et al. 2010). Tästä johtuen eri valmistajien laitteet eivät välttämättä ole toisiensa

kanssa yhteensopivia. Esineiden internetin standardien suunnittelussa tulee ottaa huomioon erilaiset rajoittavat tekijät, kuten käytössä oleva energian, verkon kapasiteetin sekä prosessointitehon rajallisuus (Bandyopadhyay & Sen 2011). Jing et al. (2014) kuvailevat standardoinnin puutteen koskevan sensorilaitteita, salausmekanismeja, avaintenhallintaa, datan tallennusformaatteja, datan prosessointimekanismeja sekä datan esittämisen kokoamista. Khan et al. (2012) puolestaan huomioivat eri laitevalmistajien tukeutuvan omiin teknologioihinsa, jolloin ne eivät välttämättä ole yhteensopivia muiden laitevalmistajien tuotteiden kanssa. Esineiden internetin teknologioiden standardisointi on välttämätön haaste, joka pitää ylittää, jotta eri valmistajien laitteet voivat toimia yhtenä isona verkostona (Khan et al. 2012). Atzori et al. (2010) ottavat kantaa tarkemmin erilaisiin teknologioihin koskien yhteyksiä laitteiden välillä, erilaisia protokollia sekä tiedonjakamista, joissa yhdistyy pieni sähkönkulutus, pieni prosessointitehon vaatimus sekä pieni verkkokaistan vaatimus. Standardoinnin puute mahdollistaa hakkereiden ja muiden pahaa haluavien tahojen hyökkäykset esineiden internetiä kohtaan, sillä monien laitevalmistajien laitteet ovat hyvin alkeellisia, eivätkä näin ollen sisällä riittävää suojausta. Tan & Wang (2010) kiteyttää esineiden internetin laajenemisen globaaliksi olevan riippuvainen standardoinnin onnistumisesta.

Yksityisyyden haaste nousee esille jo pelkästään artikkeleiden otsikoista luettuna. Yksityisyys onkin yksi suurimmista kansaa huolettavista haasteista esineiden internetissä (Tan & Wang 2010). Toisaalta suuri osa kansasta ei ole edes tietoinen omasta yksityisyydestään tai mitä tietoa heistä on missäkin järjestelmässä tallennettuna (Atzori et al. 2010; Bandyopadhyay & Sen 2011). Suurin osa yksityisyyttä suojaavista teknologioista ei ole suunniteltu rajoitettujen resurssien laitteisiin, vaan ne vaativat melko tehokasta laitteistoa toimiakseen, jollaista esineiden internet ei tarjoa käytettäväksi (Bandyopadhyay & Sen 2011). Atzori et al. (2010) ehdottavat, että yksityisyyttä tulisi suojella varmistaen, että yksityisillä henkilöillä on mahdollisuus hallita heistä kerättävää tietoa, kuka tietoa kerää ja koska tämä tapahtuu. Tietoa kerätään lähes kaikilla päivittäin käytössä olevilla laitteilla, jotka kuljettavat tietoa laitteeseen tallennettuna, minkä vuoksi niissä tulisi olla riittävä yksityisyyden suojaus ja luvaton pääsy pitäisi estää (Khan et al. 2012). Yksityisyyteen liittyy myös lain asettamat vaatimukset, jotka eivät ole vielä aivan selkeitä, kuten paikkatiedon vaikutukset ja tiedon omistajuus (Bandyopadhyay & Sen 2011; Tan & Wang 2010). Tan & Wang (2010) lisäävät yksityisyyden huomioimiseen lain ja teknologioiden lisäksi markkinoinnin sekä sosioeettisen näkökulman.

Muita kirjallisuudessa esille tulleita esineiden internetin haasteita ovat muun muassa verkon laitteiden yksilöivä nimeäminen, autentikointi, verkon turvallisuus ja avaintenhallinta. Esineiden internetin verkostossa voi olla tuhansia tai jopa kymmeniä tuhansia laitteita, joiden kaikkien tulisi olla yksilöitävissä, jolloin tarvitaan tehokasta nimeämistä ja identiteetinhallintajärjestelmää (Atzori et al. 2010; Khan et al. 2012). Järjestelmän avulla voidaan dynaamisesti osoittaa ja hallita suuren laitemäärän yksilöllisiä identiteettejä (Khan et al. 2012). Autentikointi vaatii sopivan autentikointi infrastruktuurin, jol-

laista on vaikea implementoida esineiden internetin käyttötapauksiin (Atzori et al. 2010). Ongelmaksi muodostuu esineiden internetin laitteiden resurssien minimaalisuus verrattuna muihin käytössä oleviin tietoteknisiin laitteisiin, kuten puhelimiin ja tietokoneisiin (Jing et al. 2014). Verkon turvallisuus on yhtä lailla esineiden internetin haaste, kuin se on koko internetin yleisestikin. Esineiden internetissä yhdistyy monien erilaisten verkkojen käyttö, mikä luo mahdollisuuksia epäonnistua, jos yksikin verkko on turvaton (Jing et al. 2014). Mahdollisia verkkoja ovat muun muassa langallinen ja langaton verkko, mobiiliverkot sekä ad hoc -verkot. Esineiden internetissä suuri määrä laitteita lähettää yhtäaikaisesti dataa, jolloin verkon pitää olla luotettava, jotta dataan ei pääse kukaan ulkopuolinen käsiksi ja jotta dataa ei häviä matkan varrella (Khan et al. 2012). Syitä datan muuttumiseen tai häviämiseen ovat esimerkiksi verkon ruuhkautuminen tai ulkopuolinen hyökkäys verkkoon (Jing et al. 2014). Avaintenhallinnan haasteena on sekä julkisen avaimen että salaisen avaimen siirron ja jakelun turvallisuus, jotta avaimet pysyvät vain laillisten käyttäjien tietona (Gang et al. 2011; Jing et al. 2014).

3.4 Esineiden internetin tietoturvauhkia

Esineiden internetiin liittyy monia samoja tietoturvauhkia kuin sensoriverkkoihin, mobiiliverkkoihin ja internetiin (Zhihua 2011). Tällaisia uhkia ovat muun muassa yksityisyyden suojaaminen, heterogeenisen verkon autentikointi, pääsynhallinta sekä tiedon säilyttäminen ja hallinta. Esineiden internetiin yhdistetyt laitteet ovat usein haavoittuvampia, kuin perinteisen IT:n komponentit, esineiden internetin monimuotoisuuden vuoksi, sanoo Sorebo (2015). Esineiden internetin laitteiden heterogeenisyys ja järjestelmien laaja kirjo, johtavat lisääntyneisiin tietoturvauhkiin verrattuna nykyiseen internetiin (Sicari et al. 2015). Uhat ovat aina riippuvaisia tilanteesta, jota tarkastellaan, ja vaihtelevat käytettyjen teknologioiden ja arkkitehtuurien mukaan. Uhkien tunnistaminen onkin yksilöllinen prosessi, joka tulee suorittaa jokaiselle järjestelmälle erikseen. Tässä tutkimuksessa keskitytään tunnistamaan yleisimpiä tietoturvauhkia esineiden internetille aiemmin esitellyn arkkitehtuurin mukaisesti.

Esineiden internetin tietoturvaa tulee miettiä jokaisella arkkitehtuurin tasolla, sillä eri tasoilla olevat uhat eroavat huomattavasti toisistaan. Alemmilla tasoilla uhat liittyvät pääasiassa teknisiin ratkaisuihin ja verkon turvallisuuteen, kun taas korkeammilla tasoilla puhutaan käyttöoikeuksien ja pääsynhallinnasta sekä ihmisten toiminnasta. Viitteelliseen malliin liitettynä tietoturvallisuuden tulisi huomioida ja turvata kaikki laitteet ja järjestelmät, tarjota turvallisuutta kaikille prosesseille jokaisella tasolla sekä turvata tiedonsiirto ja kommunikaatio kaikkien tasojen sisällä sekä välillä. Jing et al. (2014) ovat jaotelleet uhkia esineiden internetin tasojen perusteella havainnointitasolle, siirtotasolle sekä sovellustasolle. Heidän esittelemänsä uhat ovat hyvin tarkan tason kuvauksia, minkä vuoksi ne on liitetty ylemmän tason kategorioiden alle, yhdessä muiden lähteiden esittelemien uhkien kanssa.

Havainnointitasolla uhat liittyvät suurimmaksi osaksi käytettyihin laitteisiin (sensoreihin), niiden toimintaan ja niiden muodostaman verkoston toimintaan. Laitteiden laaja valikoima ja standardien puuttuminen muodostavat uhan, sillä kaikkien valmistajien laitteet voivat olla erilaisia toiminnaltaan ja toiminnoiltaan (Jing et al. 2014). Tästä muodostunut uhka johtuu laitteiden heterogeenisyydestä, mikä ulottuu eroavaisuuksiksi laitteiden tallennusformaateissa, turvallisuuden hallinnan mekanismeissa sekä datan prosessoinnin mekanismeissa. Laitteiden fyysinen turvallisuus asettaa myös uhan koko laitteen toiminnalle ja jopa koko verkoston alttiiksi muille uhille, mikäli laitteeseen pääsee käsiksi jokin ulkopuolinen taho (Babar et al. 2010). Tästä syystä laitteet tulisi olla suojattuja fyysisesti, mutta myös teknisesti. Laitteiden tekninen suojaamattomuus asettaa laitteet ja niiden sisältämän datan uhan alle, sillä monissa laitteissa on varsin pieni laskentateho ja tallennustila, jolloin niihin ei ole mahdollista implementoida tehokkaita suojausmekanismeja (Jing et al. 2014). Erityisesti laitteiden kuormittaminen palvelunestohyökkäyksillä on vakava uhka, joka voi pahimmassa tapauksessa kaataa koko verkoston, mikäli verkosto on heikosti toteutettu (Bandyopadhyay & Sen 2011). Myös Weber (2010) mainitsee esineiden internetin hyökkäysten kestävyyden uhaksi. Babar et al. (2010) ottaa laajemmin kantaa koko järjestelmän ympäristön turvallisuuteen, sillä koko ympäristön tulisi olla suojattu niin fyysisiltä kuin teknisiltäkin hyökkäyksiltä.

Havainnointitasolle kohdistuu lisäksi uhkia liittyen luottamukseen, yksityisyyteen sekä avainten- ja pääsynhallintaan (Jing et al. 2014). Järjestelmän luottamusta (trust) uhkaa monet, myös perinteisen internetin ongelmat, kuten salasanojen murtaminen, salakuuntelu, palvelunestohyökkäykset, tietojen väärentäminen ja uudelleenlähettäminen (Gang et al. 2011; Jing et al. 2014). Näistä monet ovat seurausta esineiden internetin rajoitetuista resursseista, mikä mahdollistaa iskut tietoturvallisuutta vastaa. Yksityisyys nousee monesti esille puhuttaessa esineiden internetistä, minkä selittää edellä mainitut uhat, minkä lisäksi yksityisyys korostuu tilanteessa, jolloin järjestelmässä käsitellään henkilöiden yksityisiä tietoja (Babar et al. 2010; Bandyopadhyay & Sen 2011; Jing et al. 2014; Weber 2010; Zhihua 2011). Uhkana yksityisyydelle on, että joku ulkopuolinen saa käsiinsä henkilöiden tietoja ja pääsee näin käyttämään niitä väärin. Yksityisyyden uhasta päästään avainten- ja pääsynhallintaan, missä uhkana on laitteiden autentikointi ja auktorisointi, avaintenjakelu ja niiden turvallinen siirto (Babar et al. 2010; Jing et al. 2014). Kaikki laitteet, jotka liittyvät verkostoon tulisi autentikoida, jotta ne ovat oikeutettuja liittymään verkostoon. Auktorisoinnilla puolestaan määritellään laitteen oikeudet toimia verkostossa (Babar et al. 2010). Näiden heikko toteutus mahdollistaa tai puuttuminen mahdollistaa järjestelmään kuulumattomien laitteiden lisäämisen osaksi verkostoa.

Siirtotasolle ominaisia uhkia ovat tiedon siirtoon liittyvät, verkkojen toimintaan vaikuttavat sekä verkkoturvallisuus (Jing et al. 2014). Siirtotason uhat vaihtelevat riippuen käytetystä verkosta, joita voivat olla langaton verkko (WiFi), 3/4G, lähiverkko (LAN), kantaverkko tai näiden yhdistelmä. Suojaamattoman langattoman verkon uhka on, että

käsiteltävään tietoon päästään käsiksi siirron aikana, jolloin sitä voidaan muokata järjestelmän huomaamatta (Jing et al. 2014). 3/4G mobiiliverkossa datan turvallisuus on uhattuna, huonon salauksen vuoksi. Lähiverkossa myös uhkana on, että joku pääsee liittymään verkkoon huomaamatta, jolloin data turvallisuus vaarantuu (Jing et al. 2014). Zhihua (2011) toteaa uhaksi kantaverkon ylikuormittumisen ja osoitteiden loppumisen kesken, kun laitteiden määrä verkostossa kasvaa riittävän suureksi. Perinteisten IP verkkojen kapasiteetti on uhattuna, mikä saattaa aiheuttaa verkon ylikuormittumisen ja edelleen vaarantaa saatavuuden (Zhihua 2011). Koko siirtotasolle kohdistuu monenlaisia verkkohyökkäyksiä, joista yleisin on palvelunestohyökkäys, jolla pyritään ylikuormittamaan verkko ja estämään sen toiminta (Babar et al. 2010; Jing et al. 2014; Weber 2010; Zhihua 2011). Bandyopadhyay & Sen (2011) toteavat, että mikäli verkko ei ole skaalautuva eli verkkokapasiteettia ei voida laajentaa tarpeen vaatiessa, aiheutuu siitä uhka verkon ylikuormittumiselle. Babar et al. (2010) sekä Weber (2010) puolestaan keskittyvät järjestelmän hyökkäysten kestävyyteen, missä uhkana ovat edellä mainitut uhat, joiden lisäksi he mainitsevat verkkoinjektiot ja verkon nuuskimisen.

Sovellustasolla monet alempien tasojen uhat toistuvat, mutta tasolla on myös ominaisia piirteitä. Sovellustason uhat ovat monesti seurausta järjestelmän toteutuksesta ja arkkitehtuurista, miten järjestelmän eri osat ja palvelut on toteutettu (Jing et al. 2014). Väärä tai turvaton data on suuri ongelma sovellustasolla, jossa datan perusteella pitäisi tehdä päätöksiä. Pääsynhallinnan toteutus korostuu, kenellä on oikeus päästä käsiksi järjestelmään ja millaiset oikeudet hänellä on tehdä muutoksia tai vaikuttaa järjestelmän toimintaan (Jing et al. 2014). Babar et al. (2010) puhuu myös tallennetun tiedon hallinnasta, missä korostuu uhat, kuten avaintenhallinnan toteutus ja luottamuksellisuuden ja eheyden säilyttäminen. Zhihua (2011) pohtii myös avaintenhallintaan liittyviä uhkia, kuten miten useiden avaintenhallintajärjestelmien välille saadaan rakennettua yhtenäinen verkko. Lisäksi hän huomauttaa arkkitehtuurin tärkeydestä koko järjestelmän kannalta, jotta tietoturvallisuus on huomioitu suunnittelusta lähtien, uhkia silmällä pitäen. Myös sovellustasolla palveluiden keskeytykset aiheuttavat uhan järjestelmän toiminnalle, mistä aiheutuu lisäksi uhka datan eheydelle, mikäli palvelu on keskeytyneenä pidempään (Jing et al. 2014). Mitä tällaisessa tilanteessa datalle tapahtuu, joka on liikkeellä jossain kohtaa järjestelmää, eikä ole vielä saavuttanut tallennuspaikkaa? Viimeisenä sovellustasoa koskettaa asiakkaiden yksityisyys, sillä sovellustasolla näitä yksityisiä tietoja käsitellään ihmisten toimesta (Weber 2010; Zhihua 2011). Uhaksi muodostuu tietoja käyttävien ihmisten toiminta, mahdolliset vahingot tiedon käsittelyssä, poistaminen ja muuttaminen. Pahimpana uhkana yksityisyydelle on kuitenkin tietojen paljastuminen tavalla tai toisella, missä kohteena voi olla esimerkiksi yrityksen tietokannassa olevien asiakkaiden maksutiedot luottokorttinumeroineen (Zhihua 2011).

3.5 Esineiden internetin tietoturvan hallintakeinoja

Esineiden internetin tietoturvallisuutta voidaan hallita lukuisilla keinoilla, joista suuri osa on hyvin teknistä taitoa vaativia. Tietoturvallisuutta voidaan toisaalta hallita myös hyvin konkreettisilla tavoilla, kuten käyttäjien kouluttamisella ja tietoturvallisuuden kommunikoimisella kaikille osallistuville tahoille (Zhihua 2011). Bauer et al. (2013) ovat listanneet esineiden internetin tietoturvallisuuden hallinnan koostuvan viidestä toiminnallisesta komponentista, jotka ovat auktorisointi, avaintenhallinta, identiteetinhallinta, autentikointi ja luottamus. Tietoturvallisuuden hallinta riippuu aina kyseessä olevasta järjestelmästä, siihen kohdistuvista uhista ja järjestelmässä käytettävästä tiedosta ja sen luonteesta. Toiseen järjestelmään riittää tietoturvallisuuden perus komponenteista koostuva hallintamalli, kun toiseen vaaditaan hyvin vahvat tietoturvan toiminnot käsittävä hallintamalli. Mitä arkaluontoisempaa järjestelmässä käsiteltävä tieto on, sitä vahvemmat suojaus toiminnot järjestelmään pitää toteuttaa. Tietoturvallisuuden hallinnan tulee pohjautua liiketoiminnan tarpeisiin ja turvata liiketoiminnan jatkuvuus.

Auktorisointi on pääsynhallinnan toiminto, jolla varmistetaan oikeudet rajoitettuihin resursseihin (Bauer et al. 2013). Auktorisoinnilla varmistetaan henkilön tai laitteen oikeudet käyttää jotain tiettyä dataa tai päästä käsiksi johonkin osaan järjestelmää. Esimerkiksi henkilöiden yksityiseen dataan tulisi päästä käsiksi vain tietoja tarvitsevien, uhkien ja vahinkojen minimoimiseksi. Auktorisoinnin tavoitteena on hallita käyttäjien oikeuksia järjestelmässä, jotta kaikilla toimijoilla on mahdollisimman niukat, mutta riittävät oikeudet toimia järjestelmässä (Bauer et al. 2013).

Avaintenhallinta koostuu avainten jakelusta ja avainrekisteristä, jossa pidetään kirjaa käytössä olevista avaimista ja niiden ominaisuuksista (Bauer et al. 2013). Avaintenhallinnan avulla mahdollistetaan kahden tai useamman laitteen välinen turvallinen kommunikaatio. Laitteet, jotka eivät ole olleet yhteydessä aiemmin tai joiden yhteensopivuus ei ole taattua, vaihtavat kommunikaation aluksi avaimia, millä varmistetaan turvallinen kommunikaatio näiden välillä. Avainten turvallinen jakelu tapahtuu pyynnöstä, jolloin avain (tai avain pari) ensin luodaan, minkä jälkeen se (ne) lähetetään turvallisesti laitteille ja tallennetaan tieto avaimen olemassa olosta rekisteriin (Bauer et al. 2013). Avainrekisterin tietojen avulla voidaan muodostaa yhteyksiä tunnettuihin laitteisiin, jolloin avaimia ei tarvitse vaihtaa useampia kertoja samojen laitteiden välisiä yhteyksiä varten.

Identiteetinhallinnalla käyttäjille luodaan yksilöivät tunnukset järjestelmään, joihin liitetään tieto käyttäjän oikeuksista järjestelmässä (Bauer et al. 2013). Identiteetinhallinnalla hallitaan kaikkien järjestelmän käyttäjien tietoja käyttäjätietokannassa. Käyttäjätietokannassa on tiedot kaikista järjestelmän käyttäjistä ja heidän oikeuksistaan toimia järjestelmässä. Identiteetinhallinnan avulla jokainen käyttäjä tunnistetaan oikeaksi käyttäjäksi, jolla on usein yksilöllinen tunnus ja salasana, joilla käyttäjä tunnistautuu järjestelmään. Jokaiselle järjestelmän käyttäjälle luodaan oma yksilöllinen identiteetti käytettä-

vään järjestelmään, jonka avulla käyttäjä tunnistautuu järjestelmään, ja jonka avulla voidaan tarvittaessa selvittää käyttäjän toimintaa (Roman et al. 2011). Käyttäjänä voi olla henkilö tai jokin esineiden internetin laite. Lisäksi jokaisella käyttäjällä on yksi pääidentiteetti, jonka lisäksi voi olla toisioidentiteettejä tai väliaikaisia identiteettejä (Bauer et al. 2013; Roman et al. 2011).

Autentikointi on osa käyttäjän ja palveluiden tunnistamista (Bauer et al. 2011). Autentikoinnin tarkoituksena on varmistaa käyttäjän oikeus käyttää palvelua, ja että käyttäjä on sallittu käyttäjä. Käyttäjä syöttää tietonsa, jotka autentikoidaan, ja joiden perusteella järjestelmä tarkistaa käyttäjän oikeellisuuden ja oikeudet järjestelmässä (Bauer et al. 2011). Autentikoinnin avulla varmistetaan, että järjestelmään ei pääse liittymään ketään sinne kuulumattomia käyttäjiä.

Luottamus on oleellinen osa esineiden internetin toiminnallisuutta, mikä määrittelee osaltaan järjestelmän tietoturvallisuutta (Roman et al. 2011). Tietoturvallisuus on luottamusta siihen, että järjestelmä toimii, kuten sen kuuluu ja siellä olevat tiedot ovat oikeita, turvassa asiattomilta ja saatavissa tarpeen vaatiessa. Luottamuksen avulla käyttäjät voivat varmistua, että heillä on järjestelmän toiminta omassa hallussaan, eikä järjestelmä hallitse käyttäjää (Roman et al. 2011). Luottamusta on vaikeaa rakentaa, sillä se on liitoksissa käyttäjään ja hänen kokemukseensa järjestelmän toiminnasta.

Tietoturvallisuuden hallintakeinot voidaan jakaa toisaalta suojaaviin, havainnoiviin ja estäviin hallintakeinoihin. Suojaavat hallintakeinot pyrkivät suojaamaan järjestelmää yleisiltä tietoturva uhilta, kuten tiedon katoamiselta ja ulkopuolisten pääsyltä järjestelmään. Suojaavia hallintakeinoja ovat esimerkiksi käyttäjien tunnistaminen ja varmuuskopiointi. Havainnoivat hallintakeinot seuraavat järjestelmän tilaa, resursseja ja toimintaa, ja pyrkivät huomaamaan muutoksia, jotka eivät ole toiminnalle hyväksyttyjä (Stoneburner et al. 2002). Havainnoivia hallintakeinoja ovat muun muassa järjestelmän monitorointi sekä hyökkäysten havainnointi. Estävät hallintakeinot pyrkivät nimensä mukaisesti estämään tietoturvallisuuden vaarantavia yrityksiä (Stoneburner et al. 2002). Estäviä hallintakeinoja ovat esimerkiksi ohjelmistojen päivittäminen, tietojen ja tietoliikenteen salaaminen sekä tietoturvallinen sovelluskehitys.

Tietoturvallinen sovelluskehitys on yksi parhaista tavoista hallita tietoturvallisuutta, sillä siinä tietoturvallisuus otetaan huomioon heti sovelluskehityksen alusta asti. Kaikki järjestelmät koostuvat ohjelmistoista, ja mikään ohjelmisto ei ole täysin tietoturvallinen. Usein ongelmana on, että tietoturvallisuus otetaan huomioon vasta ohjelmiston valmistuttua tai että se ei ole ollut mukana suunnittelusta lähtien vaatimuksena. Tietoturvallinen sovelluskehitys koostuu viidestä osa-alueesta, jotka ovat vaatimusten määrittely, suunnittelu, käyttöönotto, testaus ja kehitys (Stoneburner et al. 2002). Stoneburner et al. (2002) sanovat, että tehokkaan riskienhallinnan tulee olla integroitu osa tietoturvallista sovelluskehitystä.

4. TUTKIMUKSEN TOTEUTUS

Tässä luvussa esitellään tutkimuksen toteutukseen käytetyt menetelmät. Ensimmäisenä esitellään tiedonkeruumenetelmät, minkä jälkeen selitetään aineiston käsittely ja analyysiprosessi.

4.1 Tiedonkeruumenetelmät

Tämä tutkimus toteutettiin kuvailevana tapaustutkimuksena, koska sillä pyrittiin kuvailemaan esineiden internetin tietoturvauhkia ja niitä vastaavia hallintakeinoja. Tarkoituksena oli kuvata esineiden internetin tietoturvauhkia yleisellä tasolla ilman tarkkaa kontekstia. Löydetyt uhat ja niiden hallintakeinot pyrittiin pitämään kaikkia kontekseja koskevana, vaikka jokaista kontekstia koskee omat erityispiirteensä, joiden mukaan tietoturvauhat tulee aina määrittää yksittäisessä tapauksessa. Tutkimuksen eräänä haasteena oli se, että esineiden internetin tietoturvasta oli hyvin rajoitettu määrä kvalitatiivista lähdekirjallisuutta saatavilla, vaikka esineiden internet on ollut suuren kiinnostuksen kohteena jo useamman vuoden.

Tietoturvallisuuden lähdemateriaalia haettiin painetusta kirjallisuudesta sekä verkosta löytyneistä artikkeleista. Tietoturvallisuuden lähdekirjallisuus pohjautuu kuitenkin pääasiassa painettuun kirjallisuuteen, sillä tietoturvallisuus on aiheena sen verran vanha asia, että siitä oli löydettävissä hyvää aineistoa painettunakin. Esineiden internetin lähdekirjallisuus sen sijaan pohjautuu enemmän verkkoartikkeleihin, painetun kirjallisuuden puutteen vuoksi. Lisäksi esineiden internet kehittyy edelleen jatkuvalla tahdilla, minkä vuoksi painettu kirjallisuus on usein aikaansa jäljessä, siinä missä verkkoartikkelit ovat paremmin ajan tasalla.

Lähdekirjallisuuden haku suoritettiin käyttämällä TTY:n kirjastoa, sen artikkelihakua sekä Google Scholaria. Hakusanoja oli esimerkiksi esineiden internet, tietoturvallisuus, internet of things, information security, threat, management ja niin edelleen. Seuraavissa alaluvuissa kuvataan tämän tutkimuksen tiedonkeruu menetelmiä tarkemmin.

4.1.1 Kirjallisuuskatsaus

Tutkimuksen teoreettisen osuuden aineiston keräämiseksi suoritettiin kirjallisuuskatsaus tietoturvallisuuteen, esineiden internetiin sekä esineiden internetin tietoturvallisuuteen. Kirjallisuuskatsauksen tavoitteena oli luoda teoreettinen viitekehys tutkimuksen empiirisen osion toteuttamiselle. Tutkimuksen tavoitteena oli tunnistaa esineiden internetiä uhkaavia tietoturvauhkia ja näiden uhkien hallintakeinoja, joten ennen uhkien tunnista-

mista tulee ymmärtää mitä tietoturvallisuus tarkoittaa ja mistä osa-alueista se koostuu. Lisäksi tulee ymmärtää, mikä esineiden internet on, mitä sillä tarkoitetaan ja mistä ominaispiirteistä se koostuu. Lopuksi nämä kaksi aihealuetta yhdistetään esineiden internetin tietoturvallisuuden tutkimiseksi, jotta voidaan ymmärtää tutkimuksen aihealueen laajuus ja mittakaava.

Tutkimuksen teoreettisen osuuden eli kirjallisuuskatsauksen tekemiseksi tutustuttiin suureen määrään lähdekirjallisuutta jokaisesta osa-alueesta. Haasteena tutkimuksessa oli lähdekirjallisuuden rajallinen määrä ja aihealueiden laajuus. Molemmat tietoturvallisuus ja esineiden internet ovat melko häilyviä käsitteitä rajoiltaan, mikä vaikeutti tutkimuksen rajaamista ja aihealueiden ymmärtämistä. Kuten aiemmassa luvussa huomattiin, esineiden internetille löytyy monia määritelmiä, joista ei voida sanoa yhden olevan se oikea. Myös tietoturvallisuus on asia, joka on läsnä käytännössä kaikessa tietojärjestelmiin liittyvässä toiminnassa ja ulottuu ihmisten toiminnasta aina ohjelmien koodaukseen asti.

Kirjallisuuskatsauksessa on pyritty tekemään aihealueita yksinkertaistavia päätöksiä, sillä kumpaakaan osa-aluetta ei voitu tarkastella absoluuttisen tarkasti tutkimuksena asettamissa rajoissa. Tutkimuksessa on pyritty huomioimaan ne asiat, jotka ovat työn kannalta kaikkein merkityksellisimpiä, jotta lukija pystyy ymmärtämään työtä, sen aihetta ja tavoitteita, tuntematta aihealueita entuudestaan.

Kirjallisuuskatsaus toimii siis lähinnä empiirisen osion tukena ja antaa lukijalle valmiuden ymmärtää empiirisen osion tuloksia ja havaintoja. Seuraavassa on esitelty empiirisen tutkimuksen tekemiseen käytetty menetelmä ja toteutustapa.

4.1.2 Haastattelut

Tutkimuksen empiirinen osio toteutettiin pitämällä teemahaastatteluita asiantuntijoille puolistrukturoidun haastattelurungon perusteella (liite 1). Haastatteluita varten valmisteltiin kysymysrunko, johon oli määritelty tietyt teemat, joita seurataan. Haastatteluissa säilytettiin kuitenkin tietty avoimuus, jotta haastattelut saivat seurata haastateltavien ajatuksen juoksua sallituissa rajoissa. Haastatteluiden haasteeksi muodostui asiantuntijoiden erilainen käsitys esineiden internetistä. Jokainen haastateltava oli hieman eri mieltä mitä esineiden internetillä tarkoitetaan, mikä heijastui tietoturvauhkien määrittelyyn ja hallintakeinojen tunnistamiseen. Erityisesti hallintakeinojen tunnistaminen vaikeutui, sillä eri haastateltavilla oli erilaisia mielipiteitä uhista, jolloin tunnistetut hallintakeinot käsittelivät yleisesti nimenomaan heidän näkemiään uhkia.

Tutkimuksessa haastateltiin tilaajaorganisaation viittä asiantuntijaa kahdella eri haastattelurungolla. Lisäksi pidettiin yksi case haastattelu tilaajaorganisaation ulkopuolelta, missä tarkoituksena oli testata löydettyjä tietoturvauhkia ja niiden hallintakeinoja ulkopuolisen organisaation esineiden internetin sovellukseen. Ensimmäiset kolme haastatte-

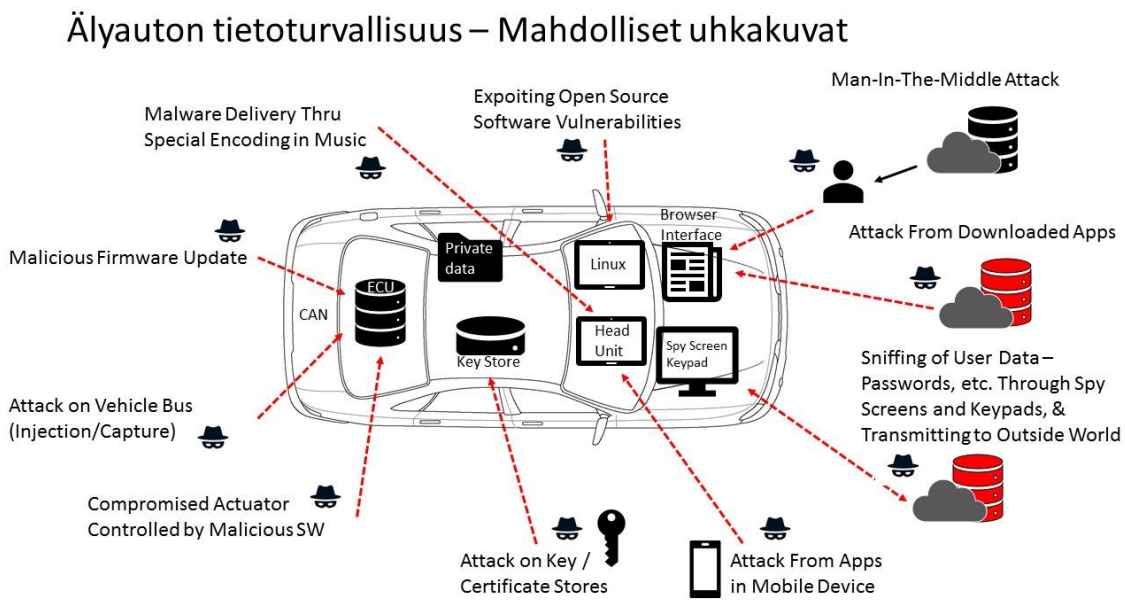
lua pohjautuivat selvittämään tietoturvauhkia esineiden internetissä ja löytämään näistä merkittävimmät asiantuntijoiden mielestä. Seuraavat kolme haastattelua käsittelivät merkittävimpien tietoturvauhkien hallintakeinoja ja niiden tehokkuutta.

Tietoturvariskien merkittävyyden ja hallintakeinojen tehokkuuden arviointi perustuu asiantuntijoiden syvään ammattitaitoon. Asiantuntijoiden keskimääräinen kokemus tietoturvallisuudesta työelämässä on 15 vuotta. Asiantuntijoiden kokemus esineiden internetistä (teollisesta internetistä) on keskimäärin 5 vuotta. Tilaajaorganisaation haastatelluista henkilöistä yksi toimii yrityksen johtokunnassa, kaksi toimii johtavina konsultteina, yksi tiiminsä esimiehenä sekä yksi teollisen internetin asiantuntijana. Tilaajaorganisaation ulkopuolelta haastateltu henkilö toimii yrityksen tietoturvapäällikkönä ja lisäksi hänellä on kokemusta monista esineiden internetin projekteista. Taulukossa 5.1 on esitelty haastateltujen henkilöiden nimikkeet organisaatiossaan, vastuualueet sekä haastattelun pidetty päivämäärä.

Taulukko 4.1. *Empiirisen aineiston keräämiseen haastatellut henkilöt*

Nimike	Vastuualue	Päivämäärä
Lead Consultant	Teollisen internetin tietoturvallisuus	9.5.2016
Lead Consultant	Ohjelmistoturvallisuus	12.5.2016
CTO	Teknologiajohtaja	18.5.2016
Zone manager	Konsultoinnin johtaminen	18.5.2016
Consultant	Teollisuusautomaation tietoturvallisuus	19.5.2016
CIO	Tietoturvapäällikkö	31.5.2016

Haastatteluissa käytettiin apuna esineiden internetin esimerkkiä, jotta haastateltavilla olisi jokin konkreettinen tartuntapinta työn laajaan aiheeseen. Esimerkkinä käytettiin älyautoa, joka on yhteydessä internettiin ja tarkkailee ympäristöään. Lisäksi suurin osa auton toiminnoista on yhteydessä auton keskustietokoneeseen, jolloin ongelma keskustietokoneessa mahdollistaa auton palveluiden käytön estymisen. Tästä esimerkkinä auton jarrujen toimimattomuus, vaikka jarrupoljinta painettaisiin. Haastatteluissa haastateltaville annettiin nähtäväksi älyauton uhkia esittelevä kuva 4.1.



Kuva 4.1. *Älyautoon kohdistuvia tietoturvauhkia*

Kuvasta 4.1 voidaan lukea useita älyautolle ominaisia tietoturvauhkia, joiden perusteella haastatteluissa pohdittiin muita mahdollisia uhkia älyautolle sekä yleisesti uhkia esineiden internetille.

4.2 Aineiston käsittely ja analyysiprosessi

Haastatteluissa kerättyä aineistoa lähdettiin avaamaan haastatteluissa apuna olleen taulukon mukaisesti, jossa uhat on järjestelty pystyakselilla luottamuksellisuuden, eheyden ja saatavuuden mukaisesti ja vaaka-akselilla esineiden internetin arkkitehtuurin tasojen mukaisesti havainnointi-, siirto- ja sovellustasoon. Taulukko 4.2 selventää tilannetta.

Taulukko 4.2. *Uhkien tunnistaminen ja kategorisointi*

	Havainnointitaso	Siirtotaso	Sovellustaso
Luottamuksellisuus			
Eheys			
Saatavuus			

Ennen haastatteluja esineiden internetin uhkia oli etsitty kirjallisuudesta ja niitä oli jaoteltu karkeasti kategorioihin. Kirjallisuudesta löydettyjen uhkien avulla haastatteluja voitiin ohjata pysymään oikeassa asiassa.

Haastatteluiden tulokset kerättiin aluksi jokaisesta haastattelusta erillisinä dokumentteina. Viimeisen haastattelun jälkeen tulokset kerättiin yhteen ja niitä jaoteltiin hieman sisällön perusteella, sillä haastatteluiden aikana kerätyt tiedot eivät olleet samalla tasolla toistensa kanssa. Osassa haastatteluista tilanteen kulku ei ollut täysin toivotun mukainen ja haastatteluista ei saatu irti toivottuja tuloksia haastateltavien taustojen ja vahvojen näkemyserojen vuoksi. Saatua aineistoa tuli analysoida jo sen keräämisessä yhteen, sillä useammista asioista puhuttiin eri nimillä, mikä aiheutti hieman lisätyötä aineiston saamiseksi vertailtavaan muotoon. Ennen haastatteluja valmistellut uhat ja hallintakeinot eivät vastanneet täysin haastatteluissa esille tulleita, minkä johdosta niitä ei voitu verrata saatuihin tuloksiin.

Haastatteluista saaduista tuloksista tehtiin taulukot, joista jätettiin tietoturvallisuuden osa-alueet pois, sillä haastateltavat eivät osanneet suoraan jaotella uhkia niiden perusteella. Uhat jaettiin esineiden internetin arkkitehtuurin osa-alueiden mukaisesti, jolloin saatiin kaikille kolmelle tasolle omat taulukkonsa, joihin kerättiin jokaisen haastateltavan maininnat uhista. Näin saatiin vertailtavat tulokset esineiden internetin uhista, joita on helppoa lukea ja joista näkee nopeasti, mitkä uhat nousivat useimmissa haastatteluissa esille.

Esineiden internetin tietoturvallisuuden hallintakeinoista saatiin haastatteluissa enemmän samanlaisia vastauksia, jolloin niistä oli myös helpompi kerätä tulokset yhteen. Hallintakeinot olivat pääasiassa helpommin ymmärrettävissä, sillä tilaajaorganisaatio tuottaa palveluita tietoturvallisuuden hallintaan. Hallintakeinot jaoteltiin kolmeen osa-alueeseen, hallintakeinon tyypin mukaisesti. Nämä osa-alueet ovat suojaavat, havainnoivat ja estävät hallintakeinot. Hallintakeinojen luokittelu samalla esineiden internetin arkkitehtuurin jaottelulla olisi ollut haastavaa ja epäselvää, sillä moni hallintakeino parantaa tietoturvallisuutta monella tasolla, jolloin käytännössä kaikki hallintakeinot olisivat olleet useassa paikassa. Tällöin merkittävien hallintakeinojen esittäminen olisi ollut haastavaa, eikä lukijalle välttämättä olisi välittynyt yhtä selkeästi, mikä oli kiinnostavinta tietoa.

Tuloksista nostettiin esille uhkia ja hallintakeinoja, jotka tuli esille useammissa haastatteluissa. Harvemmin esille tulleita uhkia ja hallintakeinoja ei avattu yhtä paljon, jolloin niiden katsottiin olevan pienemmässä osassa esineiden internetin tietoturvallisuuden hallinnassa. Tätä ei voi kuitenkaan pitää absoluuttisena totuutena, sillä uhat ja niitä vastaavat hallintakeinot ja niiden merkittävyys riippuu aina täysin tilanteesta, johon niitä sovelletaan. Työn tuloksia voidaan tästä syystä pitää yleisen tason kuvauksena mahdollisista tietoturvauhista ja niiden hallintakeinoista, esineiden internetin sovellukselle, jolloin tuloksia voidaan pitää silmällä käsiteltäessä tietyn sovelluksen tietoturvallisuuden hallintaa.

5. TULOKSET

Tässä luvussa esitellään tutkimuksen tulokset. Tulokset jaotellaan esineiden internetin tietoturvauhkiin ja tietoturvan hallintakeinoihin. Tietoturvauhat on jaettu havainnointitason, siirtotason ja sovellustason uhkiin. Hallintakeinot on jaettu suojaaviin, havainnoiviin ja estäviin hallintakeinoihin.

5.1 Esineiden internetin merkittävimmät tietoturvauhat

Esineiden internetin tietoturvauhat on jaettu tässä työssä esineiden internetin tasojen mukaisesti. Esineiden internetin tasoja ovat havainnointitaso, siirtotaso ja sovellustaso. Näillä kaikilla on tasolle ominaisia tietoturvauhkia, mutta tasoille kohdistuu myös samanlaisia uhkia, kuten palvelunestohyökkäykset. Havainnointitasolla esille nousi lähinnä teknisiin asioihin viittaavia uhkia, jotka vaativat hyökkääjältä syvällistä teknistä osaamista. Siirtotasolla uhat ovat pääsääntöisesti tietoliikenteen väliin pääsemisestä johtuvia, mikä vaatii edelleen teknistä osaamista. Toisaalta siirtotasolla korostuu myös tehdyt valinnat arkkitehtuurin suhteen, kuten miten päätelaitteita tunnistetaan ja käytetäänkö tunnistamisen apuna sertifikaatteja. Sovellustasolla uhat liittyvät datan muuttumattomuuteen ja sitä kautta datan eheyden merkitys kasvaa. Sovellustasolla korostuu myös datan yksityisyys, erityisesti mikäli data sisältää arkaluontoista materiaalia yksityisistä henkilöistä. Esimerkiksi luottokorttitietoja, henkilötietoja tai muuten henkilön yksilöiviä tietoja.

Haastatellut henkilöt on koodattu muotoon H1, H2,…H6, ja pysyvät samoina kaikissa taulukoissa. Henkilöitä H1-H5 haastateltiin esineiden internetin tietoturvauhista, henkilöitä H3-H6 tietoturvallisuuden hallintakeinoista ja siitä, millainen on tehokas hallintakeino.

Haastatteluissa on käytetty esineiden internetin sovelluksesta esimerkkinä älyautoa, jotta haastateltavilla on jokin konkreettinen tartuntapinta esineiden internetin monimuotoiseen sovelluskenttään. Esimerkillä pyrittiin konkretisoimaan tilannetta johonkin tiettyyn tilanteeseen, vaikka tulokset pyrittiin pitämään mahdollisimman yleistettävissä. Esimerkin avulla ohjattiin haastatteluita, jotta jokainen haastateltava ei puhuisi ensimmäisestä mieleen tulevasta esineiden internetin sovellusalueesta.

5.1.1 Havainnointitason tietoturvauhat

Havainnointitaso koostuu sensoreista, jotka mittaavat jotakin suuretta automaattisesti, yksittäisinä sensoreina. Mittauksen kohteena voi olla esimerkiksi lämpötila tai paine.

Sensoreista koostuu suurempi sensoreiden verkko, jonka myötä dataa kerätään suuria määriä myöhempää käyttöä varten. Tähän datan keräämiseen liittyy tietoturvauhkia, joita selvitettiin tutkimuksen haastatteluissa. Eräs haastateltava totesi datan eheyden olevan suurin uhka tällä tasolla. Hän perusteli väitettään sillä, että mikäli kerätty data ei ole eheää, saattaa se sotkea kaiken datan käytön siitä eteenpäin, jolloin data muuttuu arvottomaksi. Taulukossa 5.1 esitetään haastatteluissa esille tulleita tietoturvauhkia havainnointitasolla.

Taulukko 5.1. *Havainnointitason tietoturvauhat*

Uhka	H1	H2	H3	H4	H5
Datan väärentäminen	X	X	X	X	
Fyysinen hyökkäys		X	X	X	X
Imitointi	X	X	X		
Uudelleentoisto		X	X	X	
Palvelunestohyökkäys	X			X	
Standardien puuttuminen			X		X
Salakuuntelu			X	X	
Resurssien varastaminen		X			
Näyttämisen halu		X			
Monitoroinnin puute					X

Taulukosta 5.1 voidaan huomata, että haastatteluiden perusteella merkittävimpiä uhkia havainnointitasolla ovat datan väärentäminen, fyysinen hyökkäys, imitointi ja uudelleentoisto.

Datan väärentäminen tarkoittaa piiloutumista lailliseksi osaksi järjestelmää, jolloin hyökkääjä voi saada sensoreiden dataa käsiinsä tai peukaloida sitä. Datan väärentäminen aiheuttaa uhan tiedon eheydelle, mikä mahdollistaa suurten ongelmien syntymisen tiedon myöhäisemmässä käytössä. Datan väärentäminen mahdollistaa myös hyökkääjän soluttautumisen osaksi järjestelmää, jolloin on myös mahdollista, että sensoriverkkoon tuodaan uusi sensori, jonka avulla pystytään syöttämään virheellistä dataa palvelimelle. Suurin osa haastateltavista piti datan väärentämistä uhkana järjestelmälle. Moni haastateltavista oli kuitenkin skeptisiä datan väärentämisen todennäköisyydestä, sillä useim-

missa järjestelmissä on tarpeeksi hyvät tavat tunnistaa sensorit, mikä vaikeuttaa datan väärentämisen mahdollisuutta huomattavasti. Noin puolet haastateltavista totesivat, että datan väärentäminen vaatii hyvin teknistä osaamista ja kyseessä olevan järjestelmän ymmärrystä onnistuakseen. Kukaan haastateltavista ei kuitenkaan poissulkenut sen tapahtumisen mahdollisuutta.

Fyysistä hyökkäystä pidettiin haastatteluiden perusteella myös erittäin merkittävänä uhkana havainnointitasolla. Fyysinen hyökkäys havainnointitasolla tarkoittaa käytännössä sensoreiden fyysistä vahingoittamista tai irrottamista sensoriverkosta. Tästä aiheutuu mahdollisesti tiedon paljastumista tai haitallista seuraamista, mitkä vaarantavat tiedon luottamuksellisuuden sekä saatavuuden. Lähes jokainen haastateltava piti fyysistä hyökkäystä uhkana, vaikka sen vaikutuksista ja todennäköisyydestä oli eriäviä mielipiteitä. Osa haastateltavista piti fyysisen hyökkäyksen todennäköisyyttä uhkana lähinnä tapauksissa, joilla halutaan tarkoituksenmukaisesti tehdä vain harmia järjestelmälle. Osa haastateltavista toisaalta piti fyysistä hyökkäystä todennäköisenä, sillä sen toteutuminen ei vaadi merkittävää osaamista, sillä sensorin fyysinen rikkominen on helppoa, mikäli sensoriin pääsee käsiksi. Fyysisen hyökkäyksen todennäköisyys ja vaikutus riippuvat suuresti sensoreiden sijoittelusta ja käyttötapauksesta, tämä tuli esille monessa haastattelussa ja johti myös käytetyn esimerkin ulkopuolisiin keskusteluihin.

Imitointi koettiin haastatteluiden perusteella myös melko merkittäväksi uhaksi. Imitoinnilla tarkoitetaan laillisen sensorin identiteetin sieppaamista tai väärentämistä, minkä tavoitteena on tiedon varastaminen tai peukaloiminen. Imitointi vaarantaa tiedon luottamuksellisuuden sekä saatavuuden. Hieman yli puolet haastateltavista mainitsi imitoinnin olevan uhka esineiden internetin havainnointitasolla. Imitointia pidettiin haastatteluiden perusteella hyvin samankaltaisena kuin väärentämistä, vaikka väärentäminen koettiin hieman merkittävämmäksi uhaksi.

Uudelleentoiston haastatteluissa koki merkittäväksi uhaksi hieman yli puolet haastateltavista. Uudelleentoistaminen tarkoittaa järjestelmän luottamuksen huijaamista pääsyoikeuksien saamiseksi järjestelmään. Konkreettisesti uudelleentoistaminen on nimensä mukaisesti sensorin lähettämän viestin uudelleentoistamista. Uudelleentoistaminen vaarantaa järjestelmän luottamuksellisuuden, mikäli lähetetty viesti päätyy asiattomien käsiin, tai eheyden mikäli sensorin lähettämä viesti ei koskaan päädy järjestelmään asti. Uudelleentoistaminen vaatii syvällistä teknistä osaamista, minkä vuoksi haastateltavat eivät pitäneet sen todennäköisyyttä kovin vakavana, sen sijaan siitä mahdollisesti aiheutuvat ongelmat koettiin merkittäviksi. Muita esille tulleita uhkia on listattuna taulukossa 5.1, nämä eivät kuitenkaan olleet haastateltavien mielestä yhtä merkityksellisiä kuin ylempänä esitellyt uhat.

5.1.2 Siirtotason tietoturvauhat

Esineiden internetin siirtotasolla sensorit lähettävät keräämäänsä dataa palvelimelle jotakin tiedonsiirtotapaa käyttäen. Tason uhat riippuvat paljon käytetystä tiedonsiirtokanavasta, mutta tässä tutkimuksessa pyrittiin huomioimaan kaikki yleiset uhat tiedonsiirron yhteydessä, ottamatta kantaa käytettyyn tiedonsiirtokanavaan. Yleisimmin tiedonsiirtoon käytettään langattomia tekniikoita, kuten WLAN, 4G tai 3G yhteyksiä. Monesti käytetään myös näiden tekniikoiden sisälle rakennettuja erillisiä ominaisuuksia, esimerkiksi yksityistä APN:ää tai VPN tunnelointia. Yksityinen APN tarkoittaa omaa verkkoa palveluntarjoajan verkon sisällä, jota muut eivät näe. VPN tunnelointi taas tarkoittaa sensorin ja palvelimen välistä salattua tietoliikenneväylää. Haastatteluissa eräs haastateltava nosti saatavuuden siirtotasolla erittäin merkittäväksi, sillä mikäli jokin palvelu tai sovellus ei ole saatavilla, ei myöskään data voi siirtyä sinne tai sieltä eteenpäin. Erityisesti, mikäli päätöksenteko tapahtuu palvelimella, jossa data sijaitsee, muuttuu saatavuus kriittiseksi tekijäksi. Taulukossa 5.2 on esitelty esineiden internetin siirtotason merkittävimpiä tietoturvauhkia.

Taulukko 5.2. *Siirtotason tietoturvauhat*

Uhka	H1	H2	H3	H4	H5
Tiedonsiirron tai yhdistämisen väliin pääseminen (muuttaminen)	X	X	X	X	X
Toisena käyttäjänä esiintyminen	X	X	X	X	
Palvelunestohyökkäys	X	X	X	X	
Päätelaitteiden tunnistaminen			X	X	X
Salakuuntelu		X	X		
Uudelleentoisto		X		X	
Sertifikaatit				X	X
Arkkitehtuurin turvattomuus		X			
Ohjelmistovirheet		X			
Fyysinen uhka				X	

Taulukosta 5.2 voidaan huomata haastatteluissa esille nousseiden siirtotasolla merkittävimpien tietoturvauhkien olevan tiedonsiirron tai yhdistämisen väliin pääseminen, toisena käyttäjänä esiintyminen, palvelunestohyökkäys sekä päätelaitteiden tunnistaminen.

Tiedonsiirron tai yhdistämisen väliin pääsemistä piti kaikki haastateltavat merkittävänä uhkana. Kategoria on melko laaja käsitteeltään, sillä siinä yhdistyy sekä tiedonsiirron väliin pääseminen, että yhdistämisen väliin pääseminen. Tiedonsiirron väliin pääseminen tarkoittaa, että tiedonsiirtoa pystyttäisiin seuraamaan laittomasti tai, että tiedonsiirtoon pystyttäisiin jopa syöttämään sinne kuulumatonta dataa. Yhdistämisen väliin pääseminen tapahtuu jo ennen tiedonsiirron alkamista, jolloin yhdistettäessä sensoria palvelimelle tähän väliin päästäisiin, jolloin tietoliikennettä voidaan seurata tai muuttaa. Kategoria käsittää jossain määrin siis koko siirtotasolla tapahtuvaa toimintaa, mutta on kuitenkin ajateltu tarkoittavan tiedonsiirron yhteydessä lähinnä samankaltaista toimintaa kuin havainnointitasolla, mutta datan liikkuessa sensorilta eteenpäin palvelimelle. Tässä kohtaa uhkana on esimerkiksi tietoliikenteen uudelleentoistaminen ja identiteetin väärentäminen, joista saattaa aiheutua datan paljastumista, muuntumista tai häviämistä. Yhdistämisen kohdalla uhat ovat enemmän yhdistämisen aikaisten asioiden huomioimista, missä uhkia ovat muun muassa salakuuntelu, tiedonsiirron analysointi, tietoliikenteen estäminen ja uudelleenreitittäminen. Kategorian sisältämät uhat liittyvät kaikkiin tietoturvallisuuden osa-alueisiin luottamuksellisuuteen, eheyteen ja saatavuuteen. Uhat on selvyyden vuoksi yhdistetty tähän kategoriaan, sillä yksittäiset uhat kategorian sisällä ovat hyvin samankaltaisia ja haastateltavat puhuivat hyvin paljon samankaltaisista asioista, mutta hieman eri nimillä.

Toisena käyttäjänä esiintyminen koettiin haastatteluissa lähes jokaisen haastateltavan mielestä merkittäväksi uhaksi. Toisena käyttäjänä esiintyminen on hyvin lähellä identiteetin väärentämistä, mutta haastattelijat ottivat sen esille omana uhkanaan. Käyttäjällä tarkoitetaan tässä yhteydessä lähinnä sensoria tai palvelinta. Toisena käyttäjänä esiintyminen voidaan toteuttaa varastamalla laillisen sensorin tunnistetiedot tai imitoimalla ne, kun sensori yhdistää palvelimelle ja tunnistaminen tapahtuu. Riittävän salauksen puuttuminen aiheuttaa ongelman, mikäli joku muu voi missään vaiheessa päästä käsiksi sensorin ja palvelimen väliseen tiedonsiirtoon. Toisena käyttäjänä esiintymisestä saattaa aiheutua tiedon eheyden menettäminen tai luottamuksellisen tiedon paljastuminen.

Palvelunestohyökkäys on hyvin suoraviivainen uhka nimensä mukaisesti. Lähes jokainen haastateltava piti palvelunestohyökkäystä merkittävänä uhkana erityisesti siirtotasolla, mutta myös käytännössä jokaisella esineiden internetin tasolla. Siirtotasolla palvelunestohyökkäys konkretisoituu, kun tieto ei kuljekaan järjestelmässä ja tapauskohtaisesti saattaa aiheuttaa suuriakin vahinkoja. Esimerkiksi teollisuuden puolella palvelunestohyökkäys saattaa aiheuttaa vaaratilanteita, jos lämpötilan tai paineen muutoksista ei saadakaan reaaliaikaista dataa. Palvelunestohyökkäyksellä voidaan myös aiheuttaa harhautus jotain muuta hyökkäystä varten, jolloin jokin muu järjestelmän osa on alttiimpana hyökkäyksille. Palvelunestohyökkäykset olivat haastateltavien mielestä yksiä

yleisimpiä uhkia, joilla erilaisia järjestelmiä horjutetaan. Vaikutuksiltaan palvelunestohyökkäykset vaihtelevat suuresti pienistä järjestelmän hidastumisista aina pitkiin käyttökatkoihin ja palvelinten uudelleenkäynnistämisiin asti.

Päätelaitteiden tunnistaminen on kriittinen osa järjestelmän tietoturvallista toimintaa. Hieman yli puolet haastateltavista totesivat sen olevan merkittävä uhka siirtotasolla. Päätelaitteiden tunnistamisella varmistutaan, että vain lailliset osat järjestelmää saavat kuulua siihen, ja ettei järjestelmän osaksi pääse ulkopuolisia laitteita tai käyttäjiä. Päätelaitteiden tunnistaminen on osa järjestelmän salausta ja toimiakseen tehokkaasti, sen tulee sisältää molemminpuolisen tunnistuksen. Tällöin sekä sensori että palvelin tunnistavat toisensa ja erilaisten mekanismien myötä voivat varmistua, että toisessa päässä on laillinen järjestelmän laite. Muita esineiden internetin siirtotason tietoturvauhkia on esitettynä taulukossa 5.2 ja osa näistä liittyy edellä esiteltyihin kategorioihin, mutta ovat silti erikseen mainittavan arvoisia uhkia.

5.1.3 Sovellustason tietoturvauhat

Sovellustasolla käytetään sensoreiden lähettämää dataa hyödyksi päätöksenteon tukena. Havainnoitu tieto on lähetetty siirtotason mukaisesti palvelimelle, josta sitä tarkastellaan jonkin sovelluksen kautta. Sovellustasolle ominaista on, että käytetään jotain sovellusta datan järjestämiseksi, jolloin sitä on helpompi lukea ja käsitellä. Sovellustasolla uhkiin liittyy usein käyttäjä, sillä toiminnot eivät ole enää yhtä automatisoituja kuin alemmilla esineiden internetin tasoilla. Sovellustason merkittävimmät tietoturvauhat ovat taulukoituna alla olevassa taulukossa 5.3.

Taulukko 5.3. *Sovellustason tietoturvauhat*

Uhka	H1	H2	H3	H4	H5
Datan muuttaminen ja/tai poistaminen	X	X	X	X	
Yksityisyys	X	X	X		X
Ohjelmistojen haavoittuvuudet		X	X	X	X
Kontrollien menettäminen	X	X	X		
Fyysinen hyökkäys	X	X	X		
Palvelunestohyökkäys			X	X	X
Valvonnan puute		X	X		
Turvallisuuden vaarantuminen			X		

Pääsynhallinta					X

Taulukosta 5.3 voidaan havaita sovellustasolla merkittävimpien tietoturvauhkien olevan datan muuttaminen ja/tai poistaminen, yksityisyys, ohjelmistojen haavoittuvuudet, kontrollien menettäminen, fyysinen hyökkäys sekä palvelunestohyökkäys. Kontrollien menettäminen tuli esille erityisesti haastatteluissa käytetyn esimerkin yhteydessä puhuttaessa älyautosta. Uutisissakin esillä olleita autojen etäohjauksia ja ominaisuuksien muuttamisia on jo nyt tapahtunut, mikä nosti uhan esille haastatteluissa. Yleisesti esineiden internetin yhteydessä kontrollien menettäminen riippuu hyvin paljon käyttötapauksesta, joten sitä ei käsitellä sen tarkemmin tässä tutkimuksessa. Fyysistä hyökkäystä ja palvelunestohyökkäystä on käsitelty jo aiempien esineiden internetin tasojen uhkien yhteydessä, eivätkä ne eroa merkittävästi sovellustasolla aiemmasta, joten niiden käsittely ei ole tässä kohtaa enää tarpeellista.

Lähes jokainen haastateltavista piti datan muuttamista ja/tai poistamista merkittävänä tietoturvauhkana sovellustasolla. Datan muuntuminen koettiin hyvin kriittiseksi erityisesti, mikäli kyseisen datan perusteella tehdään päätöksiä. Esimerkiksi tehdasympäristössä lämpötilan nouseminen tietyssä prosessissa vaatii muutoksia prosessiin, jolloin väärä data saattaa aiheuttaa suuria turvallisuusriskejä ja jopa hengenvaaran työntekijöille, mikäli tehdään vääränlaisia muutoksia tai ei reagoida muutokseen mitenkään. Datan muuttumista voi tapahtua monista erilaisista syistä. Vääränlaiset konfiguraatiot järjestelmissä saattavat aiheuttaa datan menetyksiä tai ihmiset saattavat tehdä virheitä käsitellessään dataa. Yksi huolimattomuusvirhe saattaa aiheuttaa datan muuttumisen tai johtaa jopa datan katoamiseen. Haastatteluiden perusteella erityisesti ihmisten toimintaa pidettiin merkittävänä osana uhkaa. Lähes jokaisessa haastattelussa keskusteltiin työntekijöiden koulutuksen ja perehdytyksen puutteesta, mikä aiheuttaa kategorian mukaisia uhkatilanteita.

Yksityisyys korostui myös sovellustason tietoturvauhkana lähes jokaisen haastateltavan mielestä. Yksityisyyden eli esimerkiksi henkilötietojen ja maksutietojen paljastuminen asiattomille on valitettavan yleinen uhka, kun seuraa uutisia. Monet rikolliset kalastelevat yksityisiä tietoja niin yksityishenkilöiltä kuin yrityksiltäkin. Haastatteluissa nostettiin esille yksityisyyden huomioiminen kaikessa esineiden internetin toiminnassa, mutta erityisesti sovellustasolla se koettiin merkittäväksi uhaksi. Yksityisyydensuoja asettaa tallennettaville tiedoille tarkat määräykset, mutta tästä huolimatta tietoja vuotaa järjestelmien ja organisaatioiden ulkopuolelle valitettavan usein. Euroopan unionin uusi lakiasetus yksityisyydenhallinnasta tuo paljon muutoksia tietojen tallentamiseen ja käsittelyyn, minkä koettiin tuovan uusia haasteita yksityisyyden uhkakentälle.

Ohjelmistojen haavoittuvuudet korostuivat erityisesti teknisempien henkilöiden haastatteluissa, mutta huomioitiin lähes jokaisessa haastattelussa. Eräs haastateltava totesi heti

haastattelun alusta alkaen, että ”kaikki tietoturvariskit ovat seuraamusta softan huonoudesta”. Tätä hän perusteli sillä, että mikään ohjelmisto ei ole täysin tietoturvallinen ja ohjelmistoturvallisuuteen ei yleisesti panosteta riittävästi. Mikäli tietoturvallisuutta ei ole huomioitu ohjelmistokehityksen alusta alkaen, on sen parantaminen jälkikäteen hyvin vaikeaa ja resursseja vievää työtä. Ohjelmistojen haavoittuvuuksia käytetään monien muiden uhkien aiheuttamien riskien toteuttamiseen, jolloin merkitys kasvaa entisestään. Haastatteluiden perusteella ohjelmistojen haavoittuvuudet koettiin erittäin merkittäviksi uhiksi, joita ei kuitenkaan huomioida liiketoiminnassa, niiden ansaitsemalla vakavuudella.

5.2 Tietoturvallisuuden hallinnan ratkaisut

Haastatteluiden toinen tavoite oli selvittää tehokkaita hallintakeinoja tunnistetuille tietoturvauhille. Haastateltavilta H3-H6 kysyttiin tarkemmin, millainen on tehokas tietoturvallisuuden hallintakeino ja millaisia hallintakeinoja aiemmin esitellyille uhille on olemassa. Yksi haastatteluissa esille noussut huomio oli, että usein tietoturva-asiantuntijat ottavat tietoturvallisuuden hallinnan esille, mutta vasta liiketoiminta tekee tarvittavat päätökset. Tällaisissa tapauksissa kommunikaation merkitys nousee, jotta tietoturvallisuudesta ja sen tärkeydestä saadaan välitettyä viesti päättävälle organisaation tasolle. Hallintakeinojen tutkimisessa haasteeksi nousi ongelma, että hallintakeinot vaihtelevat merkittävästi riippuen kulloinkin kyseessä olevasta käyttötapauksesta. Samaa uhkaa saatetaan hallita eri tilanteissa erilaisilla hallintakeinoilla, jolloin kullekin tilanteelle tulee määritellä soveltuvat hallintakeinot erikseen kyseessä olevan uhan aiheuttaman riskin perusteella. Hallintakeinot on jaoteltu tässä tutkimuksessa haastatteluissa esille tulleiden kategorioiden mukaisesti suojaaviin, havainnoiviin ja estäviin hallintakeinoihin. Kaksi haastateltavaa pitivät edellä mainittua jaottelua hyvänä ja toimivana mallina esineiden internetin tapauksessa. Uhkien jaottelussa käytetty esineiden internetin tasojen mukainen jaottelu ei toimi hallintakeinojen yhteydessä, sillä hallintakeinot ovat usein samoja eri tasoilla esiintyville uhille. Alla olevassa taulukossa 5.4 on esitetty tehokkaan hallintakeinon ominaisuuksia, jotka tulivat esille haastatteluissa.

Taulukko 5.4. *Tehokas hallintakeino*

Ominaisuus	H3	H4	H5	H6
Uhan nopea havainnoiminen	X	X	X	X
Lokitus (jättää jäljen)		X		X
Uhan todennäköisyyden minimoiminen		X		
Jatkuva			X	

Skaalautuva, automatisoitu	X			

Tehokkaalle hallintakeinolle tunnistettiin haastatteluissa ominaisuuksiksi uhan nopea havaitseminen, lokitus, uhan todennäköisyyden minimoiminen, jatkuvuus sekä skaalautuvuus ja automatisointi. Näistä selkeästi tärkeimmäksi koettiin uhan nopea havainnoiminen, sillä kaikki haastateltavat pitivät sitä tärkeänä ominaisuutena. Toiseksi merkittäväksi ominaisuudeksi osoittautui tapahtumista pidettävä loki, jotta kaikesta toiminnasta jää jokin jälki järjestelmään, minkä perusteella voidaan etsiä uhan aiheuttajaa ja rajata se pienempään alueeseen. Yleisesti haastatteluissa todettiin, että kaikilta uhilta ei voi suojautua etukäteen, vaan tärkeämpää on uhan toteutumisen nopea havainnointi ja sen jälkeiset hallintatoimenpiteet. Eräs haastateltava totesi, että ”suojaavat toimenpiteet tulee suunnitella siten, että suojaamatta jääneiden osien aiheuttamat uhat hyväksytään”. Toiseksi hän lisäsi vielä, että ”tämän jälkeen keskiössä on uhkien nopea havainnointi, jotta niihin voidaan reagoida mahdollisimman nopeasti ja eristää uhka pienempään osaan järjestelmästä”.

5.2.1 Suojaavat hallintakeinot

Suojaavat hallintakeinot käsittävät toimenpiteet, jotka suunnitellaan merkittävimpien uhkien minimoimiseksi, jotta niitä ei pääsisi tapahtumaan. Suojaavilla toimenpiteillä pyritään tekemään järjestelmästä riittävän tietoturvallinen alusta alkaen. Hallintakeinot riippuvat aina kyseessä olevasta järjestelmästä ja sitä varten tehdystä riskianalyysistä, josta selviää juuri kyseiselle järjestelmälle tärkeimmät suojauskohteet. Tässä tutkimuksessa on etsitty mahdollisimman yleisesti päteviä hallintakeinoja, ja taulukossa 5.5 on esitelty haastatteluissa löydettyjä esineiden internetin tietoturvaa suojaavia hallintakeinoja.

Taulukko 5.5. *Suojaavat hallintakeinot*

Hallintakeino	H3	H4	H5	H6
Käyttäjien tunnistaminen	X	X		X
Laitteiden tunnistaminen	X	X		X
Avaintenhallinta	X	X		X
Varmuuskopiointi	X		X	
Varmentaminen	X			
Auktorisointi				X

Haastatteluiden perusteella tärkeimmät suojaavat hallintakeinot ovat käyttäjien tunnistaminen, laitteiden tunnistaminen ja avaintenhallinta. Käyttäjien tunnistaminen tarkoittaa nimensä mukaisesti, että kaikilla käyttäjillä on yksilölliset tunnukset järjestelmään, jolloin jokainen käyttäjä on yksilöity käyttäessään järjestelmää. Tällä hallintakeinolla voidaan varmistua, että käyttäjät ovat laillisia käyttäjiä ja ongelmatilanteessa voidaan tarkastella lokien avulla, kuka käyttäjä on tehnyt esimerkiksi virheen tai tahallisesti muuttanut tietoja vääriksi. Laitteiden tunnistaminen turvaa järjestelmän kokonaisuutta, eikä salli laittomien laitteiden liittyä osaksi järjestelmää. Laitteiden tunnistaminen suojaa järjestelmän eheyttä ja luottamuksellisuutta, pitäen järjestelmään liittyneet laitteet oikeina, jolloin ulkopuoliset eivät pääse käsiksi järjestelmään. Suurin osa haastateltavista piti sekä käyttäjien että laitteiden tunnistamista merkittävänä hallintakeinona.

Kolmantena merkittävänä suojaavana hallintakeinona haastattelijat pitivät avaintenhallintaa. Avaintenhallinta on merkittävä osa järjestelmän salausta ja jo yhden tärkeän avaimen vuotaminen saattaa merkitä koko järjestelmän luotettavuuden menettämistä. Avaintenhallinnan tarkka suunnittelu ja toteuttaminen on hyvin merkittävä osa järjestelmän salauksen varmistamista ja eräs haastateltava totesi, että ”harmittavan usein avaintenhallinta on toteutettu huonosti, eikä sitä ole välttämättä dokumentoitu millään tapaa”. Myös avaintenhallinta oli lähes jokaisen haastateltavan mielestä merkittävä suojaava hallintakeino.

5.2.2 Havainnoivat hallintakeinot

Havainnoivat hallintakeinot pyrkivät havaitsemaan järjestelmässä tapahtuvia tietoturvatapahtumia, jotta niihin voidaan reagoida mahdollisimman nopeasti. Havainnointia voidaan suorittaa monella tavalla ja havainnoitavat asiat voivat erota toisistaan huomattavasti. Monitoroinnilla voidaan seurata esimerkiksi järjestelmän käyttöasteita, verkon kuormitusta tai ohjelmien päivityshistoriaa. Lokienhallinta tarkastelee järjestelmään tehdyistä muutoksista jääviä merkintöjä, sisäänkirjautumisia sekä virheraportteja. Hyökkäysten havainnointi on tietoturvallisuuden valvontaan erikoistunut ohjelma, joka tarkkailee epäilyttäviä tapahtumia järjestelmässä, anomalioita sekä yllättäviä virheitä. Alla olevassa taulukossa 5.6 on esitelty haastateltavien vastaukset havainnoivista hallintakeinoista.

Taulukko 5.6. *Havainnoivat hallintakeinot*

Hallintakeino	H3	H4	H5	H6
Monitorointi - Tietoturva	X	X		X

- Saatavuus				
Lokienhallinta		X		X
Hyökkäysten havainnointi - Anomaliat - Virheet	X	X		

Haastatteluissa esiintyi kolmea ylemmän kategorian havainnoivaa hallintakeinoa, monitorointia, lokienhallintaa sekä hyökkäysten havainnointia. Monitorointi nähtiin normaalina toimintana, jolla seurataan järjestelmässä tapahtuvia asioita. Monitoroinnin alle löytyi tietoturvan monitorointi, joka on esimerkiksi haittaohjelmien seuraamista ja virusskannauksia. Toisena monitoroitavana asiana esiintyi saatavuus, millä tarkoitetaan järjestelmän eri osien saatavuuden seuraamista ja verkon kuormitusta. Lähes jokainen haastateltavista piti monitorointia tärkeänä hallintakeinona.

Lokienhallintaa piti haastateltavista puolet merkittävänä esineiden internetin tietoturvallisuuden hallintakeinona. Lokienhallinnan tärkeys korostuu, kun järjestelmässä tapahtuu jotain odottamatonta ja sen aiheuttajaa lähdetään selvittämään. Lokienhallinnan avulla voidaan selvittää esimerkiksi, kuka järjestelmää on tapahtumahetkellä käyttänyt tai tehnyt dataan muutoksia.

Kolmantena havainnoivana hallintakeinona haastatteluissa tuli esille hyökkäysten havainnointi. Hyökkäysten havainnointi on edistyksellinen tapa seurata järjestelmään kohdistuvia hyökkäyksiä. Hyökkäysten havainnointi toteutetaan usein omana järjestelmänään varsinaisen järjestelmän päälle ja on usein pienemmille yrityksille hyödyltään liian kallis toteuttaa. Hyökkäysten havainnointi käsittää usein järjestelmän tiedoista etsittäviä anomalioita, jotka jokin haittaohjelma tai laiton käyttäjä on voinut tehdä. Toinen yleinen järjestelmän kohde on virheiden etsiminen järjestelmästä. Virheiden myötä järjestelmästä saattaa tulla haavoittuva monille erilaisille hyökkäyksille. Hyökkäysten havainnointia piti puolet haastateltavista tärkeänä havainnoivana hallintakeinona.

Edellä mainittujen hallintakeinojen lisäksi haastatteluissa tuli hieman sivussa esille haavoittuvuusskannaukset, jotka tarkastavat järjestelmän tunnetuilta haavoittuvuuksilta, jotta niihin voidaan toteuttaa korjaavat toimenpiteet. Tätä kukaan haastateltava ei kuitenkaan nostanut sen enempää esille, joten se jätettiin pois taulukosta.

5.2.3 Estävät hallintakeinot

Estävät hallintakeinot pyrkivät nimensä mukaisesti estämään järjestelmän toimintaa vaarantavien tapahtumien realisoitumista liiketoimintaa haittaavaksi. Estävät hallintakeinot pienentävät haitallisten tietoturvatapahtumien tapahtumisen mahdollisuutta, sulkemalla yleisimpiä mahdollisuuksia pois. Estävien hallintakeinojen yksi ominaispiirre on jatkuvuus, sillä suurin osa hallintakeinoista on jatkuvaa toimintaa. Haastatteluissa estävät hallintakeinot olivat selkeästi monimuotoisimpia, minkä vuoksi haastatteluissa tuli esille useita erilaisia keinoja vain yhden tai kahden haastateltavan toimesta. Haastatteluiden lyhyen keston vuoksi ja tietoturvallisuuden laajan pelikentän luonteesta johtuen, hallintakeinojen käsittely jäi toivottua pintapuolisemmaksi. Taulukossa 5.7 on kerätty haastatteluissa esiintyneet estävät hallintakeinot.

Taulukko 5.7. *Estävät hallintakeinot*

Hallintakeino	H3	H4	H5	H6
Päivitykset	X	X	X	X
Yksityinen verkko	X	X		X
Yhteyden salaaminen (SSL, VPN)	X	X		X
Tietoturvallinen sovelluskehitys	X			X
Vain tarvittavan tiedon käsittely	X			X
Autentikointi	X			X
Koventaminen (segmentointi)			X	X
Palomuuri		X		
Skaalautuvuus		X		
Käyttäjien kouluttaminen		X		
Fyysinen turvallisuus			X	
Ajantasainen tiedon käsittely				X

Taulukosta 5.7 nähdään, että yksi hallintakeino oli kaikkien haastateltavien mielestä merkittävä, järjestelmän päivittäminen. Päivitykset ovat yksi tärkeimpiä tietoturvalli-

suudenhallinnan toimintoja, sillä mikään järjestelmä ei ole täydellinen, vaan kaikkia tulee parantaa jatkuvasti. Päivityksillä paikataan löydettyjä tietoturvauhkia, haavoittuvuuksia ja parannetaan muita ominaisuuksia, jotka saattavat myös parantaa tietoturvaa. Esimerkiksi käyttäjäkokemuksen parantaminen saattaa vähentää käyttäjien tekemiä virheitä, mikäli käyttöliittymä on yksinkertainen käyttää ja mahdollisuudet virheisiin on minimoitu.

Yksityinen verkko nousi lähes jokaisessa haastattelussa myös keskustelun aiheeksi. Yksityisellä verkolla tarkoitetaan verkkoa, joka toimii kuten mikä tahansa verkko, mutta se ei ole yleisesti nähtävillä. Haastateltavat korostivat sen toimintaa yleisenä toimenpiteenä, joka pienellä vaivalla tekee verkosta paljon turvallisemman, kun se ei ole jokaisen nähtävissä. Haastateltavien mielestä yksityisellä verkolla voidaan estää yleisimmät yritykset verkon toiminnan kaatamiseksi.

Yhteyden salaamista pidettiin haastatteluissa myös tärkeänä hallintakeinona lähes jokaisen haastateltavan osalta. Nykyään lähes kaikki vähääkään luottamuksellista tietoa käsittelevät järjestelmät käyttävät jotain salausta. Salausta on monen tasoista havainnointitasolta sovellustasolle. Haastateltavat pitivät merkittävänä erityisesti siirtotason salausta, jotta tiedonsiirron väliin ei pääse kukaan ulkopuolinen. Salaus on myös melko yleinen tapa parantaa tietoturvaa esineiden internetin järjestelmissä, vaikkakin mitä enemmän salataan tietoa, sitä enemmän se vaatii laskentatehoa laitteilta (sensoreilta), jolloin laitteiden hinnat kasvavat. Tämä aiheuttaa ongelmia, mikäli erityisesti sensoreilta vaaditaan tehoja, sillä sensoreita on järjestelmissä usein niin suuri määrä, että pieninkin hinnan nousu vaikuttaa kokonaiskustannuksiin merkittävästi.

Edellä mainittujen hallintakeinojen lisäksi taulukossa on useita keinoja, jotka ovat merkittäviä, vaikka ne eivät korostuneet useammissa haastatteluissa. Erityisesti tietoturvallinen sovelluskehitys sai korostuneen huomion, kun uhkien haastatteluissa eräs haastateltava sanoi sen olevan ”tärkein osa koko tietoturvallisuuden kehittämistä”. Hänen mielestään kaikki uhat tulevat virheistä koodissa ja koodia on kaikissa järjestelmissä. Tästä johtuen tietoturvallinen sovelluskehitys pitäisi nostaa suuremmaksi asiaksi, sillä kertaalleen huonosti tehdyn sovelluksen korjaaminen jälkeenpäin tietoturvalliseksi on todella kallista. Kaikessa sovelluskehityksessä pitäisikin hänen mielestään ottaa tietoturvallisuus huomioon heti alusta alkaen, jolloin kaikista järjestelmistä tulisi turvallisempia jo käyttöönotettaessa. Tällöinkin niitä tulee päivittää, sillä ”mikään koodi ei ole koskaan täydellistä”, hän lisäsi.

Muista maininnan arvoisia estäviä hallintakeinoja ovat vain tarvittavan tiedon käsittely järjestelmässä, autentikointi, koventaminen, palomuurit, jotka tuntuvat olevan jo itsestään selvyys sekä käyttäjien koulutus. Näistä käyttäjien koulutuksen nosti esille yksi teknisempi osaaja, mikä oli mielenkiintoista, sillä enemmän hallinnolliset asiantuntijat eivät tästä maininneet. Lopuksi voidaan mainita hieman erillisenä osana hallintakeinoja sopimustenhallinta, jonka nosti esille ainoastaan johtajan asemassa oleva henkilö. So-

pimustenhallinnalla voidaan varmistaa alihankkijoiden sitoutuminen tietoturvallisiin ratkaisuihin ja ongelmatilanteissa sopimuksiin voidaan nojata määriteltäessä vastuita.

6. POHDINTA

Tässä luvussa pohditaan tutkimuksen tuloksia. Ensimmäisenä tarkastellaan havaittuja tietoturvauhkia, sitten uhkien hallintakeinoja ja lopuksi esitellään ja analysoidaan merkittävimpiä tuloksia.

6.1 Tutkimuksen tulosten tarkastelu

Tutkimuksen teoriaosuudessa tunnistettiin esineiden internetin tietoturvallisuuden uhkia, jotka koskettavat yleisesti kaikkia esineiden internetin järjestelmiä. Jokaiselle esineiden internetin sovellusalueelle on olemassa uhkia, jotka ovat todennäköisempiä sillä, kuin jollain toisella sovellusalueella. Teoriaosuuden perusteella tietoturvallisuus on monimuotoinen kokonaisuus, joka koskettaa kaikkia ihmisiä ja verkossa toimivia järjestelmiä. Tietoturvauhat ovat konkreettisia ja niiden vaikutukset vaihtelevat tapauksesta riippuen, pienestä haitasta koko organisaation lamautumiseen. Tietoturvallisuuden hallintaan on olemassa monia tapoja, joista useimmilla voidaan hallita samanaikaisesti useampaa uhkaa. Esineiden internetin tietoturvallisuuden hallitsemiseksi tulee jokainen tilanne käsitellä yksilöllisenä, mikä tarkoittaa riskikartoituksen tekemistä jokaisesta erillisestä tilanteesta. Tässä työssä tunnistetut uhat ja hallintakeinot ovat kirjallisuudessa usein esiintyneitä sekä haastatteluissa useimmiten esille tulleita. Tässä tutkimuksessa tunnistettuja uhkia ja hallintakeinoja ei kuitenkaan voida pitää yleisimpinä uhkina tai hallintakeinoina, sillä tutkimuksen otos on varsin pieni ja kattaa vain yhden toimialan asiantuntijoiden näkemyksen. Lisäksi tutkimukseen osallistui yksi toisen toimialan ammattilainen, joka hänkin oli perehtynyt tietoturvallisuuteen työtehtävänsä puolesta. Tämän otoksen perusteella voidaan todeta haastattelu havaintojen olevan tässä tutkimuksessa vaikuttavia tekijöitä teorian ohella. Haastatteluissa tunnistetut uhat koettiin tärkeiksi, sillä niiden koettiin aiheuttavan suuria ongelmia toteutuessaan. Tällä tarkoitetaan, esimerkiksi koko järjestelmän rikkoutumista tai vakavaa tietojen vuotamista. Mitä vakavamman ongelman uhka toteutuessaan aiheuttaa, sitä tärkeämmäksi se koettiin haastatteluissa. Hallintakeinojen tärkeys puolestaan selittyi näiden vakavien uhkien hallitsemisella. Toinen hallintakeinon tärkeäksi määrittelevä asia oli, kuinka moneen uhkaan hallintakeino vastaa. Useimmat hallintakeinot auttavat useamman kuin yhden uhan hallitsemisessa, joten tärkeimmiksi koetut hallintakeinot hallitsevat yhtä tai useampaa vakavaa uhkaa.

6.1.1 Tietoturvauhkien tarkastelu

Teoria- sekä empiriaosuuden perusteella on havaittavissa, että tietoturvauhkia on olemassa todella paljon, ja teknologian kehittyessä niitä tulee jatkuvasti lisää. Empiriaosuudessa tietoturvauhat jaettiin esineiden internetin arkkitehtuurin tasoille, jolloin saatiin parempi käsitys, missä kohtaa järjestelmää uhka sijaitsee. Uhkia tunnistettiin useampia arkkitehtuurin alemmilla tasolla, mikä selittyy tasojen ja uhkien teknisyydellä. Mitä korkeammalle arkkitehtuurin tasolle siirrytään, sitä enemmän uhat kohdistuvat inhimillisiin tekijöihin, teknisten sijaan. Monet uhat liittyvät tekniseen toteutukseen ja siellä piileviin heikkouksiin ja virheisiin. Teoria ja empiria osoittivat hallintakeinoista monenlaisia syventymistasoja hallintakeinojen esittämiseen, minkä vuoksi erityisesti teoria syventyy monesti hyvin tekniselle tasolle empirian jäädessä pintapuolisemmaksi tarkasteluksi. Toisaalta empirian tavoitteena ei ollut saada teknistä tarkastelua uhista eikä hallintakeinoista vaan ennemmin yleisemmän tason uhkia ja hallintakeinoja.

Empiirinen osuus jakautuu haastatteluissa löydettyihin esineiden internetin uhkiin ja uhkien hallintakeinoihin. Uhkia tarkastellessa empiriassa esiintyi paljon niin sanottuja uhkien yläkäsitteitä, kuten identiteetinhallinta ja yksityisyys. Teoria osuudessa sen sijaan uhkia käsiteltiin useasti hyvin teknisistä näkökulmista ja esiteltiin uhkien syntymistä teknologioiden perusteella. Teoria nosti esille paljon teknisiin asioihin liittyviä uhkia ja käsitteli niitä hyvin syvällisesti, mikä ei ollut tämän tutkimuksen kannalta merkityksellisintä. Tutkimukselle merkityksellisintä tietoa oli yleisemmät kuvaukset millaisia tietoturvauhkia ja niiden hallintakeinoja yleisesti on tunnistettavissa esineiden internetille. Monet lähteet puhuivat esimerkiksi verkko- sekä tiedonsiirtoteknologioista, joiden syvällinen tutkiminen ei kuulunut tämän työn laajuuteen. Empiirinen osuus pyrki vastaavasti tunnistamaan näitä uhkia, riippumatta käytetyistä teknologioista. Empiirisessä osuudessa painoarvo oli yleisesti pätevien uhkien tunnistamisessa ja niiden yhteydestä esineiden internetin arkkitehtuurin osa-alueeseen. Mielenkiintoista empiirisessä osuudessa oli haastateltavien näkemyserot ja koko esineiden internetin määritelmän ymmärtäminen. Tämä tuli hyvin esille myös tutkimuksen teoriassa, missä esiteltiin useita määritelmiä esineiden internetille. Haastateltavien erilaiset käsitykset esineiden internetistä voivat johtua esineiden internetin tuntemattomuudesta, sen poikkeavista käyttötarkoituksista tai erilaisista kokemuksista. Vastaajilla voi olla hyvin erilaisia kokemuksia ja tietoja esineiden internetistä ennen tutkimusta, jolloin he saattoivat määritellä sen mielessään heille ensimmäisenä tulevan mielleyhtymän perusteella. Useammassa haastattelussa tuli myös esille, että asioita muistui hiljalleen eri kohdissa haastattelua, jolloin haastattelussa jouduttiin hieman hyppimään eri osioiden välillä. Tämä kertoo aiheen olleen vaikea haastateltaville ja sen, että haastateltavat eivät työnkuvastaan johtuen olleet valmistautuneet haastatteluun erityisemmin. Toisaalta myös yrityksen taustat ja tutkimuksen aikaiset projektit saattoivat määrittää haastateltavien ajatuksen kulkua ja tuoda yhtymiä sen hetkisistä ajatuksista. Esineiden internet ei ole yksiselitteinen ilmiö ja sovellusalueiden laajuus luo haasteen sen määrittelemiseen, kuin myös sen tietoturvalli-

suuden määrittelemiseen ja uhkien tunnistamiseen. Yllättävää oli, että haastatteluissa jokaiselle esineiden internetin arkkitehtuurin tasolle tunnistettiin kolmesta neljään uhkaa, jotka nousivat esille lähes kaikissa haastatteluissa. Ennen haastatteluja olisi voinut kuvitella, että jollekin tasolle olisi tunnistettu enemmän uhkia kuin jollekin toiselle. Uhkien jakautuminen näin tasaisesti yllätti tutkijan, sillä teoriassa uhat sijoittuivat enemmän arkkitehtuurin alemmille tasoille, ollen näin teknisiä. Tästä voidaan päätellä, että haastateltavat eivät olleet yhtä teknisesti orientoituneita kuin teorian asiantuntijat. Sen sijaan haastateltavat toimivat pääosin konsultointi tehtävissä, minkä seurauksena useimmat heidän tekemänsä ratkaisut ovat tekniikan ja inhimillisten tekijöiden yhdistelmiä, eli kattavat koko arkkitehtuurin. Tällä on saattanut olla vahvakin vaikutus siihen, että uhkia tunnistettiin jokaiselta tasolta lähes yhtä paljon. Jokaiselle tasolle tunnistettiin myös uhkia, joita mainitsi vain yksi haastateltavista.

6.1.2 Tietoturvallisuuden hallintakeinojen tarkastelu

Empiirisen osuuden toisessa osassa käsiteltiin hallintakeinoja yleisesti ja pyrittiin aluksi tunnistamaan, millainen on tehokas hallintakeino. Tehokkaalle hallintakeinolle tunnistettiin haastatteluiden perusteella yksi ominaisuus, joka nousi esille jokaisessa hallintakeinoja käsitelleessä haastattelussa. Tällainen ominaisuus oli uhan nopea havaitseminen, mistä voidaan päätellä, että kaikkien uhkien torjuminen tai niiltä suojautuminen ei ole tietoturvallisuuden hallinnassa tärkeintä, vaan ennemminkin se, että uhka havaitaan mahdollisimman nopeasti. Miksi tällaiseen havaintoon päädyttiin, löytyy mahdollisesti yrityksen sisältä. Yrityksessä vallitseva ilmapiiri on, että tuntemattomien uhkien havaitseminen on liiketoiminnallisesti kannattavampaa kuin niiltä suojautuminen. Tämän uskon olevan totta, sillä tietoturvajärjestelmiä erilaisiin tarkoituksiin on todella paljon ja niistä edistyneimmät vaativat erittäin suuria investointeja. Tämä johtaa siihen, että monilla pienemmillä yrityksillä ei ole edes mahdollisuutta investoida sellaiseen. Jolloin havainnointi on selkeästi kannattavampaa useimmissa tapauksissa, jolloin vasta uhan realisoituessa voidaan alkaa korjaaviin toimenpiteisiin. Tällöin säästytään ylimääräisiltä investoinneilta, joiden tarpeellisuutta on vaikea määrittää, ellei uhkia ole ennalta havaittu toteutuvan. Esineiden internetin osalta uhan nopea havaitseminen on vieläkin suuremmassa roolissa, sillä käsiteltävä data on usein reaaliaikaista, jolloin pienetkin häiriöt saattavat aiheuttaa dominoefektin myötä suuria ongelmia. Esineiden internetin tapauksessa kaikilta uhilta suojautuminen tai niiden estäminen on lisäksi lähes mahdotonta verkostojen laajuuden ja prosessointikapasiteetin rajoitteellisuuden vuoksi. Uhan nopea havaitseminen mahdollistaa uhan eristämisen nopeasti, jolloin sen mahdollisesti aiheuttamat vahingot voidaan rajata nopeasti pieniksi. Yksittäinen tällainen havainnointitapa on esimerkiksi kokonaisvaltainen järjestelmän monitorointi. Mitä järjestelmässä tapahtuu ja onko jokin järjestelmään tuleva arvo normaalista poikkeava? Tällaisia tietoja ei teoria osuudesta löytynyt, sillä teoria käsitteli enemmän vain suoraan tunnistettujen uhkien hallintaan käytettäviä keinoja. Hallintakeino on tehokas silloin, kun se seuraa jatkuvasti järjestelmän toimintaa ja mukautuu tilanteeseen sen muuttuessa. Toisaalta hal-

lintakeino ei ole tehokas, mikäli se ei turvaa järjestelmää miltään tunnistetulta uhalta, jolloin voidaan puhua hallintakeinosta, joka on ylimääräinen tai ei muutoin sovi kyseisen järjestelmän turvaamiseen. Tällainen tilanne voi olla esimerkiksi, mikäli jotain liiketoiminnallisesti merkityksetöntä järjestelmää turvataan erittäin kalliilla hyökkäysten havainnointi järjestelmällä. Käytännössä tällaisia tilanteita ei kuitenkaan juurikaan maailmalta löydy, sillä tietoturvallisuudelle on usein, jos ollenkaan budjetoitu hyvin vähäiset resurssit yritysliiketoiminnan maailmassa.

Esineiden internetin tietoturvallisuuden hallintakeinot jaettiin eräässä haastattelussa esille tulleen jaon perusteella suojaaviin, havaitseviin ja estäviin hallintakeinoihin. Teoriassa Stoneburner et al. (2002) esittelivät samanlaisen jaon, joka vahvistui aidosti käytetyksi haastatellun tietoturva-asiantuntijan kokemuksen perusteella. Jaottelu oli tutkimuksen kannalta mielekäs, sillä hallintakeinojen jakaminen arkkitehtuurin perusteella olisi tehnyt hallintakeinojen ymmärtämisestä monimutkaista, sillä useat hallintakeinot olisivat esiintyneet jokaisella tasolla. Jaon perusteella hallintakeinoja on helpompi ymmärtää ja mieltää millainen mikäkin hallintakeino on. Esineiden internetin tapauksessa jako toimi mielestäni hyvin, sillä se oli selkeä, ymmärrettävä ja hallintakeinojen sijoittaminen oli suhteellisen loogista tämän jaottelun perusteella. Havainnoiva hallintakeino kertoo jo itsessään, että sillä ei pyritä hallitsemaan varsinaisesti mitään uhkaa, vaan tunnistamaan tapahtuva tilanne nopeasti, jotta sen jälkeen sitä voidaan hallita. Hyvä suojaava hallintakeino on sellainen, mikä lisää järjestelmän suojausta pitämällä järjestelmään pääsyn riittävän vaikeana ulkopuolisille. Hyvänä esimerkkinä toimii käyttäjien ja laitteiden tunnistaminen ja esimerkiksi salasanalle asetettujen vaatimusten lisääminen (pituus, erikoismerkit). Havaitseva hallintakeino on tehokas, silloin kun se pystyy havaitsemaan ja jopa ilmoittamaan käyttäjälle reaaliajassa järjestelmässä tapahtuvasta toiminnasta, joka poikkeaa normaalista. Estävän hallintakeinon tehokkuus perustuu järjestelmässä olevien tietoturvareikien minimointiin. Esimerkiksi sovellusten päivittäminen korjaa aiemmin löytyneitä heikkouksia, jolloin järjestelmä pysyy ajan tasalla, eikä sisällä vanhoja tunnettuja heikkouksia.

Teoriassa monet uhat olivat teknisiä, jolloin niiden hallintakeinot ovat myös teknisiä ratkaisuja. Toisaalta teoriassa huomattiin, että tietoturvallisuuden hallinta on vain 20 prosenttia teknisiä ratkaisuja ja 80 prosenttia hallinnollisia ratkaisuja. Tämän tiedon perusteella tässä tutkimuksessa havaituilla uhilla ja hallintakeinoilla pystytään vastaamaan vain hieman yli kahteenkymmeneen prosenttiin, sillä tutkimuksessa korostuivat teknisemmät uhat ja hallintakeinot. Teknisten uhkien korostuminen on seurausta hyvin teknisesti orientoituneista haastateltavista sekä heidän laajasta tekniikoiden hallinnastaan. Lisäksi esineiden internet aiheena tuntui johdattavan haastateltavia enemmän tekniikkaa kuin käytäntöä kohti. Hallinnollisia uhkia ovat esimerkiksi käyttäjien toiminnasta aiheutuvat ongelmat. Käyttäjien toiminta voi olla tahallista tai tahatonta. Useimmiten käyttäjät eivät ole tietoisia tietoturvariskeistä, eivätkä tämän vuoksi osaa niiltä varautua. Hallinnolliset hallintakeinot koostuvat kaikesta, mikä ei sisällä teknisiä ratkaisuja, kuten

tietoturvapolitiikat, käyttäjien kouluttaminen ja salassapitosopimukset. Tutkimuksessa ei korostunut ihmisten toiminta, joka on teorian valossa kuitenkin yksi suurimpia tietoturvauhkia niin yleisesti kuin esineiden internetissäkin.

Hallintakeinojen tunnistaminen empiirisessä osuudessa onnistui lähes yhtä hyvin kuin uhkien tunnistaminen. Mielenkiintoista oli, että yhdeltä haastateltavalta saadut tulokset olivat hyvin niukkoja verrattuna muihin haastateltaviin. Häneltä saatiin vain muutama vastaus jokaiselle tasolle, kun muilta saatiin selkeästi useampia. Kyseessä oli juurikin esineiden internetiin syventynyt haastateltava, minkä vuoksi saadut tulokset hämmästyttivät. Haastateltava ei ollut yhtä perehtynyt tietoturvallisuuteen kuin muut vastaaja, mutta silti hänen vastauksensa olivat hyvin pitkälti samanlaisia kuin muidenkin haastateltavien. Haastateltava jäi selkeästi muita enemmän miettimään juurikin esineiden internetille spesifejä uhkia, mikä lopulta näkyi ajan rajallisuuden vuoksi saatujen tulosten määrässä. Toisaalta saadut vastaukset saattavat olla parempia kuin muiden vastaajien, ottaen huomioon hänen asiantuntijuutensa esineiden internetiä koskien. Yleisesti ottaen haastateltavilta saatiin hyvin tuloksia ja tulokset olivat enimmäkseen samanlaisia. Kuitenkin erityisesti estäviin hallintakeinoihin löytyi useampia hallintakeinoja, joita tuli esille vain yhdessä haastattelussa. Hallintakeinoista, kuten uhistakin, nousi kahdesta kolmeen vastausta, jotka lähes kaikki haastateltavat mainitsivat. Syitä samanlaisille vastauksille ovat niiden yleisyys tietoturvallisuudessa ylipäätään sekä haastateltavien taustat. Monet esille nousseista uhista ja hallintakeinoista ovat hyvin yleisiä aina puhuttaessa tietoturvallisuudesta. Esimerkkinä uhista palvelunestohyökkäykset sekä yksityisyys ja hallintakeinoista päivitykset sekä käyttäjien tunnistaminen. Nämä hallintakeinot ovat hyvin linjassa teorian kanssa, vaikka hallintakeinojen syvällisyys saattaa jonkin verran vaihdella teorian ja empirian välillä. Empiriassa suojaavien hallintakeinojen yhteydessä nousi useimmiten esille käyttäjien tunnistaminen ja laitteiden tunnistaminen, jotka ovat molemmat teoriassa yhden hallintakeinon alla. Teoria painottaa selkeästi enemmän suojaavia ja estäviä hallintakeinoja suhteessa havainnoiviin. Empiriassa kuitenkin aluksi todettiin havainnoimisen olevan yksi tärkein ominaisuus hallintakeinossa. Tätä voidaan selittää sillä, että yleisesti katsottuna on vaikeaa sanoa, miten uhkia voi havainnoida, ottamatta kantaa mihinkään tiettyyn tilanteeseen. Tämän vuoksi empiria tuo myös uusia näkökulmia teorian vierelle.

Tutkimuksessa oli alun perin tarkoitus myös arvioida uhkien vaikutuksia ja merkittävyyttä, mutta tämä osoittautui heti haastatteluiden aluksi olevan käytännön tasolla todella vaikeaa. Ensimmäinen haastateltava totesi jo, että merkittävyyden määrittelemiseksi tulisi tietää uhan todennäköisyys ja vaikutus, mitkä riippuvat täysin tilanteessa käsiteltävästä tapauksesta tai järjestelmästä, jolloin se tulisi tuntea tarkasti. Tutkimuksessa käytettiin esimerkkinä älyautoa, jotta vastauksiin saatiin lisättyä konkreettinen tapaus. Merkittävyyden määrittely oli tästäkin huolimatta vaikeaa, sillä haastateltavat takertuivat, teoriassa voimakkaasti esille tulleisiin, tarkkoihin käytettyihin teknologioihin ja niiden vaikutuksiin. Haastatteluiden puitteissa haastateltavilla ei ollut aikaa perehtyä

älyauton teknologioihin pintapuolta tarkemmin, minkä vuoksi uhkien todennäköisyyden arvioiminen oli heidän mielestään mahdotonta. Lisäksi vaikutuksen arviointi riippuu muista järjestelmistä, joita älyauton tapauksessa käytetään auton ulkopuolella, joista ei myöskään ollut tarkempaa tietoa saatavilla. Merkittävyyttä päätettiin perustella sen sijaan haastatteluissa useimmiten esiintyneiden vastausten mukaisesti, jolloin mitä useampi vastaaja puhui samasta uhasta tai hallintakeinosta, pääteltiin sen olevan tämän tutkimuksen valossa merkittävämpi. Tässä huomioitiin myös teoriassa esiintyneet havainnot, joita haastatteluiden tulokset täydentävät. Tämä tapa ei kuitenkaan ole tällä otannalla täysin pätevä, vaikka haastateltavat ovat alansa ammattilaisia. Merkittävyyden sijaan tulosten voidaan sanoa olevan tässä tutkimuksessa yleisimpiä. Haastatteluiden ja teorian perusteella tunnistetut yleisimmät esineiden internetin tietoturvallisuuden hallintakeinot on esitetty taulukossa 6.1.

Taulukko 6.1. *Yleisimmät hallintakeinot haastatteluiden perusteella*

Hallintakeinot	Vastausten määrä (max 4)
Ohjelmistopäivitykset, patchit	4
Poikkeamien havainnointi (valvonta, lokitus, anomaliat)	3
Tietoturvallinen kehitysprosessi (secure SDLC, salausalgoritmit, Open SAMM)	3
Verkon segmentointi (yksityinen verkko)	3
Yhteyden salaaminen (VPN, SSL)	3
Molemminpuolinen oikeellisuuden varmistaminen (sertifikaatit, auktorisointi)	3
Sensoreiden luottamuksellisen datan minimointi	3
Fyysinen suojaus	3

Taulukossa 6.1 on kerätty yhteen empiriassa tunnistettujen hallintakeinojen vastausten lukumäärät, joista vain ohjelmistopäivitykset nousivat esille kaikissa hallintakeinoja käsittelevissä haastatteluissa. Syynä tähän on hallintakeinojen määrän laajuus, joita haastattelujen rajallisuuden vuoksi ei ehditty tarkastella laajemmin. Pidemmillä haastatteluilla ja tarkemmalla älyauton kuvaamisella sekä älyautoon liittyvien teknologioiden ja järjestelmien tuntemuksella olisi varmasti saatu parempia tuloksia. Haastateltavien

vastauksissa korostamista hallintakeinoista oli huomattavissa heidän erikoisosaamisensa. Sovelluskehitykseen erikoistunut asiantuntija korosti erityisesti tietoturvallisen sovelluskehityksen tärkeyttä, kun taas tietoturvallisuuden havainnoinnin asiantuntija tunnisti enemmän havainnointiin liittyviä hallintakeinoja. Haasteena hallintakeinojen kirjaamisessa oli, että monessa haastattelussa puhuttiin samoista asioista hieman eri nimityksillä ja abstraktiotasoilla. Monet haastateltavista puhuivat suoraan joistain tietyistä tavoista toteuttaa hallintaa, kuten verkon salaamiseen käytettävästä VPN tai SSL salauksesta. Tästä syystä taulukossa esiintyy konkreettisia esimerkkejä hallintakeinon sisältävistä ratkaisuista. Kaikki taulukon esimerkit ovat haastateltavien mainitsemia, minkä jälkeen niitä on analysoitu hallintakeinoihin yhdistämiseksi. Ohjelmistopäivitysten jälkeen seuraavat seitsemän yleisintä hallintakeinoa mainittiin kaikki kolmessa haastattelussa ja taulukossa esitetty järjestys on oman tulkintani mukainen yleisyys.

6.2 Merkittävimpien tulosten analysointi

Tutkimuksen teoria ja empiirisessä osuudessa tunnistettiin monia uhkia jokaiselle esineiden internetin arkkitehtuurin tasolle, minkä lisäksi näille tunnistettiin mahdollisia hallintakeinoja. Seuraavassa on tehty analyysiä uhista, niiden mahdollisista seurauksista, niitä vastaavista hallintakeinoista sekä tietoturvallisuuden osa-alueista, jotka uhka vaarantaa. Uhat on tunnistettu teorian ja empirian yhdistelmän perustella ja ne on luokiteltu yleisiksi haastatteluiden perusteella. Perusteena yleisyydelle on ollut haastatteluissa vastaajien lukumäärä, eli kuinka moni haastateltava otti esille uhan, miten he niitä perustelivat ja mitkä he kokivat näistä yleisimmiksi. Keskusteluissa jotkin esille otetuista uhista todettiin hyvin yksityiskohtaisiksi, jolloin analyysin perusteella niitä ei luokiteltu yleisesti esineiden internetin tietoturvallisuuden merkittäviksi uhiksi. Seuraukset on saatu pääasiassa pohdinnan ja teorian yhteistyönä ja ovat hyvin geneerisiä. Seuraukset vaihtelevat suuresti kyseessä olevan järjestelmän, sen arkkitehtuurin, ratkaisujen ja siellä olevan tiedon kriittisyyden mukaan, minkä vuoksi tässä tutkimuksessa ei voitu todeta tarkkoja seurauksia, sillä tutkimuksessa ei ollut riittävän tarkasti määriteltyä tutkittavaa kohdetta (järjestelmää).

Uhkia vastaavat hallintakeinot ovat seurausta empiirisestä osuudesta, jolloin haastateltavat pohtivat millaisilla keinoilla tiettyjä uhkia voitaisiin hallita. Tietoturvallisuuden osa-alueet ovat jälleen pohdinnan ja analyysin tulosta ja edelleen uhkien kohteiden puuttuessa, ne voivat useassa tapauksessa koskettaa useampaa osa-aluetta. Lopulta vastaajien lukumäärä kuvastaa haastatteluissa uhan maininneiden haastateltavien lukumäärää, minkä perusteella uhkien merkittävyyttä on analysoitu. Taulukossa 6.2 on esitetty tutkimuksen merkittävimpien tulosten yhteenveto, missä yhdistetään tutkimuksen perusteella merkittävimmät uhat, niitä vastaaviin hallintakeinoihin. Lisäksi taulukossa on omaa pohdintaa sekä teorian ja empirian yhdistelmää edellä mainituilla tavoilla.

Taulukko 6.2. *Merkittävimpien tulosten yhteenveto*

Esineiden internetin taso	Uhka	Seuraus	Hallintakeino	Tietoturvallisuuden osa-alue	Vastaajien lkm (max 5)
Havainnointi	Datan väärentäminen	Datan menettäminen, muuttaminen, väärän datan syöttäminen	Identiteetinhallinta, laitteiden autentikointi	Luottamuksellisuus, eheys	4
Havainnointi	Fyysinen hyökkäys	Tiedon paljastuminen, sensorin menettäminen	Laitteiden ja tilojen fyysinen suojaaminen, luottamuksellisen datan minimointi laitteessa	Luottamuksellisuus, eheys, saatavuus	4
Havainnointi	Imitointi	Datan paljastuminen tai muuttaminen	Langattoman tiedonsiirron salaus, sertifikaatit	Luottamuksellisuus	3
Siirto	Tiedonsiirron tai yhdistämisen väliin pääseminen (muuttaminen)	Tiedonsiirron analysointi, tiedon paljastuminen, muuttuminen	Salaus, autentikointi, avaintenhallinta, sertifikaatit, yksityinen verkko	Eheys	5
Siirto	Palvelunesto-hyökkäys	Palvelun käyttö estyy, päätöstenteko estyy	Pääsynhallinta, verkon salaus, verkon reititysprotokolla	Saatavuus	4
Siirto	Toisena käyttäjänä esiintyminen	Tiedon paljastuminen, muuttuminen, katoaminen, ohjaus väärään paikkaan, pääsy liiketoimintakriittisiin tietoihin	Pääsynhallinta (auktorisointi), verkon salaus	Luottamuksellisuus	4
Sovellus	Yksityisten tietojen vuotaminen	Tiedon paljastuminen, brändin heikkeneminen	Varmuuskopiointi, tietojen salaaminen, tietoturva-arkkitehtuuri	Luottamuksellisuus	4
Sovellus	Datan muuttaminen ja/tai poistaminen	Datan muuttuminen ja/tai katoaminen, liiketoiminnan häiriöt	Molemminpuolinen oikeellisuuden varmistaminen (sertifikaatit, auktorisointi)	Eheys	4
Sovellus	Ohjelmiston haavoittuvuudet	Minkä tahansa uhan realisoituminen ja sen seuraukset	Tietoturvallinen kehitysprosessi, ohjelmistopäivitykset	Luottamuksellisuus, eheys, saatavuus	3

Taulukossa 6.2 uhkien hallintakeinoista löytyy kaikki aiemmin mainitut yleisimmät hallintakeinot, sillä jo pelkästään niiden avulla voidaan suojautua useimmilta tietotur-

vauhilta. Perusteluna tälle on, että nämä yleisimmät hallintakeinot ovat niin kattavia, että suurin osa yleisimmistä uhista on niiden avulla hallinnassa. Vaikka tietoturvauhkia on kaikkialla, ovat yleisimmät niistä teknisesti hyvin yksinkertaisia ja järjestelmiä vastaan usein käytettyjä. Jo näiden hallintakeinojen käyttöönotto suojaa järjestelmää suurimmalta osalta yleisimmistä uhista ja hyökkäyksistä. Erityisesti tietoturvallinen kehitysprosessi käsittää kaikkien järjestelmien kehittämisen ja niissä tietoturvallisuuden huomioimisen alusta alkaen. Eräs haastateltava argumentoi käytännössä koko haastattelun kaikki vastauksensa sillä, että kaikki tietoturvauhat ovat seurausta huonosta ja virheellisestä ohjelmistokoodista jossain kohtaa järjestelmää. Lisäksi hän totesi, että ohjelmistokoodi ei ole koskaan täydellistä ja turvallista, jolloin aina löytyy tietoturva-aukkoja, joita voidaan hyödyntää järjestelmää vastaan. Inhimillisetkin uhat hän selitti sillä, että ohjelmistojen koodi ei pysty suojaamaan käyttäjän tekemiltä virheiltä täydellisesti. Muihin hallinnollisiin uhkiin ja erityisesti käyttäjiin liittyviin, hän ei tarkemmin ottanut kantaa. Mielestäni mikään ei ole näin mustavalkoista, vaikka osaltaan hän on oikeassa, että monet uhat ovat pohjimmiltaan peräisin ohjelmistokoodin epätäydellisyydestä. Käyttäjien toimintaa ei kuitenkaan voida selittää tällä, vaan se pitää huomioida omana osanaan. Sama henkilö totesi myös, että ei nähnyt esineiden internetin tietoturvallisuuden eroavan juurikaan perinteisen IT:n tietoturvallisuudesta. Hänen mukaansa esineiden internet koostuu samaan tapaan tietokoneista ja tietoverkoista, joissa piilee samat tietoturvauhat kuin perinteisen IT:n järjestelmissä. Tätä kohtaan tulee kuitenkin olla hieman skeptinen, sillä esineiden internet voidaan yksinkertaistetusti nähdä, kuten hän sen näkee, mutta käytännössä esineiden internet sisältää myös paljon sille ominaisia piirteitä. Näistä voidaan mainita esimerkiksi automatisoinnin taso ja kerätyn tiedon automaattisen analysoinnin perusteella tehtävät analyysiin perustuvat toiminnot. Tulosten perusteella voidaan sanoa, että tietoturvauhilta ei voi koskaan suojautua täysin, mutta käyttämällä merkittävimpien hallintakeinojen listausta hyväksi, voidaan yleisesti ottaen suojautua monilta yleisimmiltä esineiden internetin tietoturvallisuuden uhilta.

Tutkimuksen päätutkimuskysymyksenä oli ” Miten esineiden internetin tietoturvauhkia voidaan hallita tehokkaasti?” Vastaus tähän löytyy sekä teoriasta että empiriasta. Teorian perusteella tietoturvallisuuden hallinta lähtee riskianalyysistä, jolloin tunnistetaan organisaatioon tai sen johonkin järjestelmään kohdistuvat riskit. Riskien tunnistamisessa tulisi myös arvioida jokaiselle riskille vaikutus ja todennäköisyys, joiden määritteleminen ei onnistunut tämän tutkimuksen yleisellä tasolla. Tästä syystä tutkimuksessa puhutaan uhista eikä riskeistä. Peltier et al. (2005) määrittelivät perinteisen riskienhallinta prosessin kappaleessa 2.4, mutta tämän tutkimuksen perusteella prosessia on hieman päivitettävä. Tämän tutkimuksen perusteella mukautettu tehokas prosessi hallita riskejä (uhkia) on suunnitella toiminta, havainnoida toimintaa, puuttua havaittuun toimintaan mahdollisimman nopeasti ja estää samanlaisten tapahtumien tapahtuminen jatkossa. Tällä perusteella tunnistetuista uhista määritellään ne, joilta halutaan ehdottomasti suojautua. Muiden tunnistettujen uhkien seuraukset hyväksytään sillä tasolla, että kunhan niiden konkretisoituminen havaitaan, niin niihin voidaan puuttua nopeasti. Mikäli jokin

uhka toteutuu useasti tai sen seuraukset muuttuvat kriittisemmiksi liiketoiminnan kannalta, voidaan sitä varten suunnitella jatkossa estävät toimenpiteet ja ottaa ne käyttöön. Optimitilanteessa suojaudutaan vain tarvittavilta ja liiketoiminnallisesti kriittisimmiltä uhilta ja muiden tunnistettujen uhkien seuraukset hyväksytään sillä tasolla, että ne tunnistetaan ja että niiden seuraukset voidaan minimoida nopeasti tarvittaessa. Uhkia tulee tarkkailla jatkuvana prosessina, sillä uhat muuttuvat jatkuvasti, ja tarpeen mukaan ottaa käyttöön lisää tietoturvallisuutta parantavia toimintatapoja ja/tai järjestelmiä.

Tutkimuksen tuloksilla saatiin tutkimuskysymysten mukaisesti tunnistettua esineiden internetin uhkia ja hallintakeinoja. Hallintakeinoista saatiin luotua tutkimuksen rajallisuuden puitteissa merkittävimpien hallintakeinojen listaus, jota voidaan käyttää yleisenä työkaluna tietoturvallisuuden suunnittelun apuna. Merkittävimmät hallintakeinot ovat ohjelmistojen päivittäminen, poikkeamien havaitseminen järjestelmässä sekä alusta alkaen tietoturvallinen sovelluskehitys. Päivitysten tärkeys tulisi olla nykyään jo oletusarvo, sillä päivittämättömät sovellukset ja järjestelmät ovat usein tietoturvattomia monellakin tavalla. Poikkeamien havaitseminen liittyy tietoturvan ja liiketoiminnan yhdistämiseen, jolloin tehokkaalla havainnoinnilla voidaan välttyä turhilta investoinneilta järjestelmiin, jotka eivät palvele liiketoiminnallisia tarpeita. Tietoturvallinen sovelluskehitys on vielä useassa tapauksessa utopiaa, sillä panostus tietoturvallisuuteen pitäisi tehdä heti kehityksen alkuvaiheessa, jolloin sitä ei tarvitsisi korjata koko sovelluksen loppukäyttöikää. Käytännön tasolla investointi tietoturvalliseen sovelluskehitykseen kannattaa, sillä se tulee tehokkaammaksi kuin sovelluksen esimerkiksi viidentoista vuoden käyttöiän tietoturvallisuuden ylläpitäminen ja kehittäminen.

Haastatteluissa monet haastateltavat olivat hyvinkin eri mieltä mitä esineiden internet tarkoittaa ja miten tietoturvauhkia voidaan tunnistaa yleisesti, ilman tiettyä kohdetta. Eräs haastateltava sanoi, ettei uhkia voi tarkastella ilman määrättyä kohdetta, minkä johdosta hänen vastauksensa päättyivät enemmän avoimiin kysymyksiin haastattelijaa kohtaan, että voiko näin edes tehdä. Tuloksilla toisaalta ei saatu arvioitua uhkien vaikutuksia tai todennäköisyyksiä, sillä ne ovat riippuvaisia käsiteltävästä kohteesta. Lisäksi tuloksilla ei voida varmistua merkittävyyden oikeellisuudesta tai luotettavuudesta, sillä haastateltavien määrä oli suhteellisen pieni, ja edelleen yleisesti on vaikeaa määritellä, mikä on merkittävää, kun tiedossa ei ole kohteen tarkkoja tietoja. Esimerkiksi kohteessa käsiteltävä tieto ja sen käytettävyyden muoto vaikuttavat suuresti uhan merkittävyyteen.

7. PÄÄTELMÄT

Tässä luvussa esitellään tutkimuksen päätelmät. Ensimmäisenä esitellään tutkimuksen johtopäätökset ja tärkeimmät havainnot. Seuraavaksi analysoidaan työtä ja sen onnistumista ja lopuksi ehdotetaan mahdollisia jatkotutkimusideoita.

7.1 Tutkimuksen johtopäätökset

Tutkimuksen päätutkimuskysymyksenä oli ”Miten esineiden internetin tietoturvauhkia voidaan hallita tehokkaasti?” Tätä kysymystä selvitettiin aluksi teoriassa, missä kysymys jaettiin palasiksi, jolloin tutkittiin tietoturvallisuutta, esineiden internetiä sekä uhkien hallintaa. Tämän jälkeen empiirisessä osiossa selvitettiin, millaisia uhkia esineiden internetiin liittyy, millaisilla hallintakeinoilla niitä voidaan hallita sekä millainen on tehokas hallintakeino. Mielenkiintoista kysymyksen selvittämisessä oli huomata, kuinka erilaisia asiantuntijoiden käsitykset eri käsitteistä ovat ja kuinka he reagoivat kysymyksiin, jotka eivät olleet heille helppoja vastata. Esineiden internetin käsitys oli monella erilainen, mikä heijastui heidän vastauksiinsa ja edelleen tutkimuksen tuloksiin. Esineiden internetin tarkempi esittely ja tässä tutkimuksessa käytetyn määritelmän avaaminen olisi ollut hyödyllistä. Tehokkaan hallintakeinon määritteleminen osoittautui hankalaksi, sillä tehokkuus riippuu yleisesti hyvin paljon kyseessä olevasta uhasta sekä tilanteen muista osatekijöistä. Lisäksi hallintakeinojen yksilöiminen tiettyyn uhkaan osoittautui haasteelliseksi, sillä yhdellä hallintakeinolla voidaan hallita useita erilaisia ja tasoisia uhkia, joskaan yksi hallintakeino ei välttämättä anna täyttä turvaa edes yhtä uhkaa kohtaan. Kokonaisuudessaan kysymykseen saatiin kuitenkin kattava vastaus, joka sisältää tunnistettuja yleisiä uhkia, niiden lajittelun esineiden internetin tasoille, tehokkaan hallintakeinon ominaisuudet, tunnistettuja hallintakeinoja sekä niiden lajittelun hallinnan luonteen perusteella. Kiinnostavinta oli huomata, että on mahdotonta sanoa mitkä ovat yleisesti tärkeimmät uhat ja miten niitä voidaan hallita tehokkaasti, sillä tietoturvallisuus on yksilöllistä jokaisessa tapauksessa. Jokaiseen tapaukseen liittyy erilainen ympäristö, erilaiset teknologiat, erilaiset toimintatavat ja –prosessit sekä erilainen johtamistyyli. Nämä kaikki luovat yhdessä kyseessä olevan tapauksen toimintaympäristön, joka on aina erilainen, jolloin yleisesti tunnistetut uhat ja hallintakeinot ovat hyvin mahdollisia useimmissa tapauksissa, mutta niitä ei voida silti pitää suorana vastauksena minkään tilanteen hallitsemiseksi. Edellä mainitun lisäksi tulee huomioida tarkemmin myös ihmisten toiminta osana järjestelmää. Ihmisten toiminnan arviointi ja siinä piilevät uhat jäivät tutkimuksessa melko pienelle painoarvolle, vaikka teoriassa niitä pidettiin kuitenkin suuressa arvossa. Teoriassa esiteltiin tulos, jonka perusteella jopa 80 prosenttia tietoturvallisuuden hallinnasta on hallinnollisia eli ihmisiin liittyviä ratkaisuja. Mielestäni

tämä kertoo hyvin perinteisestä tietoturvallisuuden ajattelumallista, joka on toisaalta viimeisten vuosien aikana muuttunut radikaalisti. Aiemmin tietoturvallisuus käsitettiin teknisenä asiana, mistä myös tämän tutkimuksen tulokset kertovat. Nykyään tietoturvallisuus kuitenkin on enemmän yksittäisten käyttäjien, ihmisten, valintoja ja toimintaa sekä niistä aiheutuvia uhkia. Tämän tutkimuksen haastatteluissa keskustelu oli tästä huolimatta hyvin teknistä, minkä saattoi aiheuttaa myös esineiden internetin pitäminen teknisenä sekä haastateltavien tekniset taustat.

Päätutkimuskysymystä tarkennettiin alatutkimuskysymyksillä, joista ensimmäinen on ”Mitä tietoturvauhkia esineiden internetiin liittyy?” Tätä kysymystä tarkasteltiin teoriassa, mistä löytyi paljon tietoturvauhkia, joista kuitenkin suurin osa oli teknisiin ratkaisuihin viittaavia. Kirjallisuudesta ei löytynyt juurikaan tietoa esineiden internetin tietoturvasta, eikä löytyneet artikkelit ottaneet yleisellä tasolla kantaa uhkiin tai niiden vakavuuteen. Monet artikkelit keskittyivät johonkin tiettyyn teknologiaan, jolla jokin yksittäinen tapaus on toteutettu tai yleisesti syvällistä teknistä ymmärrystä vaativiin ongelmakohtiin esineiden internetissä käytetyissä teknologioissa. Tämän vuoksi kysymystä tarkennettiin myös haastatteluissa, jolloin haastateltavat pääsivät arvioimaan heidän mielestään merkittäviä uhkia. Teorian ja empirian yhdistelmänä saatiin muodostettua käsitys yleisesti merkittävimmistä tietoturvauhista. Merkittävin havainto uhista oli, että suurin osa tunnistetuista uhista oli teknisiä, eikä niinkään hallinnollisia. Mielenkiintoista kuitenkin oli, että teoriassa Kyrölä (2001) sanoi, että 80 prosenttia tietoturvallisuudesta on hallinnollisia ratkaisuja ja vain 20 prosenttia teknisiä ratkaisuja, mikä sotii tutkimuksen havaintoja vastaan.

Toinen alatutkimuskysymys oli ”Mitkä tietoturvauhat ovat merkittävimpiä esineiden internetissä?” Tähän kysymykseen vastattiin empiriassa, jossa haastateltavien vastauksien perusteella pääteltiin, mitkä uhat ovat merkittävimpiä. Merkittävyyttä pääteltiin haastateltavien vastausten lukumäärän sekä heidän argumentaationsa perusteella. Mielenkiintoisinta oli huomata, kuinka osa haastateltavista jäi pohtimaan vain uhkien riippuvuutta tilanteesta, jolloin heidän vastauksensa jäivät hieman vajaiksi. Haastateltaville tuotti vaikeuksia arvioida yleisesti merkittävimpiä uhkia, sillä osa haastateltavista korosti erityisesti uhkien riippuvuutta tilanteesta, jolloin he eivät osanneet vastata, mitkä olisivat yleisesti merkittävimpiä. Tästä huolimatta jokaiselta arkkitehtuurin tasolta nousi muutama uhka lähes jokaisessa haastattelussa, minkä perusteella niitä voidaan tämän tutkimuksen valossa pitää yleisesti merkittävimpinä uhkina.

Viimeinen alatutkimuskysymys oli ”Millaisilla hallintakeinoilla esineiden internetin tietoturvauhkia voidaan hallita tehokkaasti?” Tähän kysymykseen vastattiin empirian perusteella, missä haastateltavat pohtivat uhille hallintakeinoja ja niiden tehokkuutta. Hallintakeinoille löytyi haastatteluista hyvä lajitteluperuste, jota työssä käytettiin. Hallintakeinojen tunnistaminen osoittautui helpommaksi kuin uhkien tunnistaminen, minkä lisäksi hallintakeinot olivat helpompia mieltää yleisesti päteviksi. Mielenkiintoisinta oli erään haastateltavan kommentti, että esineiden internetin tietoturvallisuuden hallinta on

sama asia kuin minkä tahansa IT-järjestelmän hallinta, sillä esineiden internet on perinetisistä järjestelmistä koostuva verkosto. Esineiden internet on vain paljon suuremman mittakaavan järjestelmä, jolloin hallinta on siinä mielessä hankalampaa ja työläämpää. Hallintakeinoista nousi myös jokaisesta luokasta muutama hallintakeino, jotka koettiin tehokkaimmiksi ja joilla voidaan suojautua mahdollisimman monelta uhalta.

Kokonaisuutena tutkimuskysymyksiin vastattiin kattavasti, vaikkakin monet kysymyksistä oli vaikeita siinä mielessä, että tutkimuksessa ei ollut mitään konkreettista tilannetta, johon vastaukset olisi voinut kohdistaa. Tämä oli muutenkin tutkimuksen vaikein osa, ottaen lisäksi huomioon, että sekä tietoturvallisuus että esineiden internet ovat hyvin laajoja kokonaisuuksia. Lisäksi molempien suurien aihealueiden määritelmät ovat hieman liukuvia, jolloin niin allekirjoittanut kuin haastateltavatkin olivat ajoittain kysymyksen äärellä, että miten aihealue määritellään ja mitä kaikkea se sisältää.

7.2 Tutkimuksen ja tulosten arviointi

Hyvän tutkimuksen olennaisena osana on myös tutkijan oma arviointi, jonka perusteella voidaan arvioida tutkimuksen toteuttajan omaa kriittistä arviointia tutkimuksen onnistuneisuudesta ja uskottavuudesta (Olkkonen 1994, s. 111). Tämä tutkimus tuntuu varsin onnistuneelta tutkimuskysymysten ja niihin vastaamisen perusteella, vaikka uskottavuus ja yleistettävyys jäävät hieman kyseenalaisiksi.

Tämä tutkimus oli ymmärtävä kvalitatiivinen tutkimus, jonka lopputuloksena syntyi priorisoitu listaus esineiden internetin yleisistä tietoturvauhista sekä uhkien hallintakeinoista. Tunnistetut uhat vaikuttivat yleisesti tunnustetuilta ja vastaavasti tunnistetut hallintakeinot olivat valideja. Ymmärtävänä tutkimuksena tavoitteena oli luoda yleinen kuvaus esineiden internetin tietoturvauhista ja hallintakeinoista. Tämä tavoite saavutettiin, vaikka haastatteluissa tuli moneen kertaan esille, ettei uhkia voi todeta varmaksi ilman konkreettista tapausta.

Tutkimuksen yleistettävyyttä voidaan kyseenalaistaa, sillä kuten mainittua, jokaiseen tapaukseen liittyy omat uhkansa, eikä uhkia voi täysin yleistää jokaiseen tapaukseen. Luotettavuus voidaan myös nostaa esille, sillä tutkimuksessa haastateltiin vain kuutta asiantuntijaa. Tämä haastateltavien määrä ei anna täysin oikeaa kuvaa tunnistettujen uhkien ja hallintakeinojen listauksista, sillä jotain on saattanut jäädä huomaamatta ja asiantuntijoille ei välttämättä ole tullut kaikki asiat mieleen lyhyen haastattelun aikana. Tästä huomiona haastatteluissa ja koko tutkimuksessa korostuneet tekniset tietoturvauhat ja hallintakeinot. Haastateltavilla oli myös hyvin erilaisten taustat, mikä vaikutti selkeästi heidän vastauksiinsa. Teknisesti hyvin asiantuntevat haastateltavat tunnistivat nopeasti monia tekniikkoihin liittyviä uhkia ja hallintakeinoja, mutta inhimilliset uhat jäivät todella vähälle painoarvolle. Toisaalta haastatteluissa käytetty esimerkki, älyauto, oli myös teknisempään asiaan viittaava, eikä auton tapauksessa usein ole mahdollista, että käyttäjä saisi esimerkiksi auton joitain tietoja poistettua, mikä johtaisi jarrujen toi-

mimattomuuteen. Toisenlaisella esimerkillä inhimilliset uhat olisivat saattaneet tulla merkittävämmin esille teknisten rinnalle. On myös mahdollista, että esineiden internetissä tietoturvauhat kohdistuvat enemmän teknisiin kuin hallinnollisiin toimijoihin. Myös käsitykset esineiden internetistä vaihtelivat ja loivat oman haasteensa tutkimukselle. Yleisesti voidaan todeta, että tutkimuksen aihe koostui kahdesta valtavasta osa-alueesta, tietoturvallisuudesta ja esineiden internetistä, mikä vaikeutti tutkimuksen tekoa, mutta myös saatujen tulosten luotettavuutta. Samasta syystä tutkimuksen tuloksissa ei ole saatu tunnistettua kaikkia uhkia, saati hallintakeinoja.

Tutkimusta ja haastatteluita suoritti vain yksi henkilö, mikä vaikutti myös osaltaan tutkimuksen luotettavuuteen. Tutkimuksen subjektiivisuuteen vaikutti tutkijan omat tietoturvauhkien kategorisoinnit sekä niiden käyttö haastatteluiden tukena. Haastatteluissa pyrittiin seuraamaan haastattelurunkoa ja toimimaan subjektiivisesti, mutta aiheen vaikeuden vuoksi tässä ei täysin onnistuttu. Muutamassa haastattelussa olisi ollut tarpeen selittää tarkemmin tutkittava tilanne sekä toivottujen tulosten luonne.

Tutkimuksen laajuus vaikuttaa myös rajoittavasti tulosten luotettavuuteen. Diplomityön laajuuden puitteissa ei ole mahdollista tutustua kaikkiin mahdollisiin tutkimuksen aihetta käsitteleviin tutkimuksiin. Tästä syystä on mahdollista, että joitakin tutkimuksen kannalta merkityksellisiä artikkeleita on jäänyt huomaamatta. Toisaalta suoraan tätä tutkimusta vastaavia artikkeleita ei käytännössä kirjallisuudesta löytynyt ja suurin osa artikkeleista oli hyvin teknologiakeskeisiä, mikä vähentää tätä riskiä.

Tuloksissa ei juurikaan huomioitu, että tietoturvallisuuden ratkaisuissa tulee aina miettiä ratkaisujen hintaa suhteessa suojattavaan tietoon. Kaikkea ei ole järkevää tai edes mahdollista suojata, usein resurssit rajoittavat hyvin paljon mahdollisia käytössä olevia ratkaisuja. Tämän vuoksi tuloksissa esitellyt hallintakeinot eivät aina ole parhaita, kun otetaan huomioon ratkaisun hinnan suhde saatuihin hyötyihin. Usein tilanne on, että suojattavia kohteita on ylimäärin, mutta niistä pitää löytää liiketoiminnallisesti tärkeimmät, joihin saatavilla olevilla resursseilla voidaan toteuttaa mahdollisimman tehokkaat hallintakeinot. Tietoturvallisuus on siis tasapainottelua riittävän tehokkaan suojauksen toteuttamisessa, mahdollisimman pienillä resursseilla.

7.3 Jatkotutkimusideat

Tutkimukseen aiheen tarkastelu tässä tutkimuksessa on pintapuolinen ja antaa suuntaa aiheen syvemmälle tarkastelulle. Aihetta ei lähestytty minkään yksittäisen esineiden internetin osa-alueen kannalta, minkä vuoksi jokaiselle osa-alueelle voisi olla tunnistettavissa yksilöllisempiä uhkia ja hallintakeinoja. Tietoturvauhkia voitaisiin tutkia tarkemmin ja liittää niihin syitä, jotka johtavat uhkaan sekä seurauksia uhan realisoitumisesta. Myös jokaisen yksittäisen esineiden internetin osa-aluetta voisi tutkia paljon tarkemmin, millainen tietyn osa-alueen tietoturvallisuus on, mitä ominaisuuksia sillä on sekä millaiset uhat tiettyä osa-aluetta koskettaa ja miten niitä voidaan hallita.

Tietoturvallisuuden hallintakeinoja voitaisiin tutkia tarkemmin ylipäätänsä, sillä yleisiä hallintakeinoja löytyi kirjallisuudesta melko niukasti. Tästä syystä niiden esittely myös teoria osuudessa jäi selkeästi vähemmälle. Hallintakeinojen tarkastelun yhteydessä merkittäväksi hallintakeinoksi nousi päivitykset, joiden arvoa ei voi väheksyä. Kuten eräs haastateltava asian muotoili, ovat kaikki uhat seurausta ihmisten tekemistä ohjelmistovirheistä, joita päivityksillä paikataan hitaasti. Tästä syystä jatkossa olisi hyödyllistä kohdistaa tutkimusta tietoturvallisuuden huomioimiseen heti sovelluskehityksen alusta alkaen. Tällä voidaan välttää monet hyvin kalliit korjaukset sovelluskehityksen myöhäisessä vaiheessa tai sovelluksen/järjestelmän ollessa jo markkinoilla tai operatiivisessa toiminnassa.

Sovelluskehityksen näkökulmasta perinteinen IT ja esineiden internet rakentuvat molemmat ihmisten luomista järjestelmistä, jotka ovat tietoturvauhkia täynnä. Tietoturvallisuuden näkökulmasta esineiden internet on vain paljon monimutkaisempi ja laajempi perinteisen IT:n järjestelmä, johon vaikuttaa samat lainalaisuudet kuin mihin tahansa järjestelmään. Tämän tutkimuksen tulosten perusteella työtä esineiden internetin tietoturvallisuuden parissa on vielä paljon, mutta laajempaa tarkastelua voitaisiin kohdistaa erityisesti ihmisten toiminnan kehittämiseen niin sovelluskehityksessä kuin valmiin järjestelmän käyttämisessä. Lisäksi tutkimus millaiset uhat esineiden internetissä ovat vaikuttavampia, tekniset vai inhimilliset, olisi mielenkiintoinen, sillä tämän tutkimuksen valossa inhimilliset uhat tuntuivat jäävän täysin teknisten uhkien taakse.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Tietosanoma Oy. Tallinna. 291 s.

Ashton, Kevin. 2009. That ”Internet of Things” Thing. RFID Journal. Viitattu 24.8.2016. Saatavissa: http://www.rfidjournal.com/articles/view?4986

Atzori, L., Iera, A. & Morabito, G. 2010. The Internet of Things: A Survey. Computer networks. doi:10.1016/ j.comnet.2010.05.010. 19 s.

Babar, S., Mahalle, P., Stango, A., Prasad, N. & Prasad, R. 2010. Proposed security model and threat taxonomy for the internet of things (IoT). Communications in Computer and Information Science. Vol. 89. ss. 420-429.

Bandyopadhyay, D. & Sen, J. 2011. Internet of Things: Applications and Challenges in Technology and Standardization. Wireless Personal Communications. Vol. 58. Is. 1. ss. 49-69.

Bassi, A., Europe, H. & Horn, G. 2008. Internet of Things in 2020. Road Map for the Future. Viitattu 24.8.2016. Saatavissa: http://www.smart-systems-integration.org/public/documents/publications/Internet-of-Things_in_2020_EC-EPoSS_Workshop_Report_2008_v3.pdf.

Bauer, M., Boussard, M., Bui, N., Carrez, F., Jardak, C., De Loof, J., Magerkurth, C., Meissner, S., Nettsträter, A., Olivereau, A., Thoma, M., Walewski, J.W., Stefa, J. & Salinas, A. 2013. Internet of Things – Architecture (IoT-A). Deliverable D1.5, Final architecture reference model for the IoT v3.0. IoT-A 257521. 482 s.

Brotby, W.K. 2009. Information security management metrics. A Definitive guide to effective security monitoring and measurement. CRC Press. 211 s.

Bruner, Jon. 2013. Industrial Internet – The Machines Are Talking. California, USA. O’Reilly. 50 s.

Cearley, D., W. 2016. Top 10 Technology Trends for 2016. Forbes, Tech. Viitattu 26.2.2016. Saatavissa: http://www.forbes.com/sites/gartnergroup/2016/01/15/top-10-technology-trends-for-2016/2/#4eca12665830

Chen, Yen-Kuang. 2012. Challenges and Opportunities of Internet of Things. Proceedings of the 17th Asia and South Pacific Design Automation Conference (ASP-DAC). Sydney, Australia. ss. 383-388.

Chui, M., Löffler, M. & Roberts, R. 2010. The Internet of Things. McKinsey Quarterly 2. ss. 1-9.

Ericsson. 2014. Machine-to-machine: Exploring Potential Operator Roles. Viitattu 24.8.2016. Saatavissa: https://www.ericsson.com/res/docs/whitepapers/wp-m2m.pdf.

Foster, Andrew. 2015. Messaging Technologies for the Industrial Internet and the Internet of Things Whitepaper – A Comparison Between DDS, AMQP, MQTT, JMS, REST, CoAP and XMPP. Version 2.0. Messaging Technologies Whitepaper. PrismTech Corporation. 26 s.

Gang, G., Zeyong, L. & Jun, J. 2011. Internet of Things Security Analysis. 2011 International Conference on internet Technology and Applications. ss. 1-4.

GSMA. 2014. IoT Device Connection Efficiency Guidelines. Viitattu 24.8.2016. Saatavissa: http://www.gsma.com/connectedliving/wp-content/uploads/2016/04/TS-34-v3-0v2.pdf.

Gupta, S. & Hirdesh, A. 2007. Overview of M2M. Ankit Hirdesh Papers. Viitattu 24.8.2016. Saatavissa: http://sites.google.com/site/hridayankit/M2M_overview_paper.pdf.

Hakala, Juha, T. 2006. Informaatiohyöky – Tiedon ja osaamisen hallinta työelämässä. Helsinki. Gaudeamus Kirja / University Press Finland Ltd. 264 s.

Haller, Stephan. 2010. The Things in the Internet of Things. Paper presented at the Internet of Things Conference, 5.10.2010. Tokyo, Japan.

Haller, S., Karnouskos, S. & Schroth, C. 2008. The Internet of Things in an Enterprise Context. Toim. Dominique, J., Fensel, D. & Traverso, P. Future Internet – FIS 2008. New York, USA. Spinger Berlin-Heidelberg. ss. 14-28.

Halminen, Laura. 2016. Poikkeuksellinen kyberhyökkäys onnistui sammuttamaan ukrainalaisten sähköt. Helsingin Sanomat. Viitattu 14.3.2016. Saatavissa: http://www.hs.fi/ulkomaat/a1452053903722

Henry, Kevin. 2004. Risk management and analysis. Tipton, H & Krause, M. (toim.) Information security handbook. 5. painos. Boca Raton, CRC Press. ss. 751-758.

ISO/IEC 17799:2000. 2000. Code of practice for information security management. Geneva, Switzerland. International Standards Organization.

ISO/IEC 27001:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Suomen Standardisoimisliitto SFS. 66 s.

ISO/IEC JTC 1. 2014. Internet of Things (IoT) – Preliminary Report 2014. Geneva, Switzerland. International Standards Organization. 11 s.

ITU-T. 2012. Internet of Things Global Standards Initiative. Viitattu 31.8.2016. Saatavissa: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

Jing, Q., Vasilakos, A.V., Wan, J., Lu, J. & Qiu, D. 2014. Security of the internet of things: Perspectives and challenges. Wireless network. Vol. 20. ss. 2481-2501.

Kaario, K. & Peltola, T. 2008. Tiedon hallinta – Avain tietotyön tuottavuuteen. 1. painos. Jyväskylä. WSOYpro / Docendo-tuotteet. 164 s.

Kaplan, Ray. 2004. A Matter of trust. Tipton, H & Krause, M. (toim.) Information security handbook. 5. painos. Boca Raton, CRC Press. ss. 727-740.

Khan, R., Khan, S.U., Zaheer, R. & Khan, S. 2012. Future Internet: The Internet of Things Architecture, Possible Applications and Key Challenges. Proceedings – 10th International Conference on Frontiers of Information Technology, FIT 2012. IEEE. ss. 257-260.

Krco, S. & Carrez, F. 2014. Designing IoT Architecture(s): A European perspective. 2014 IEEE World Forum on Internet of Things (WF-IoT). ss. 79-84.

Krutz, R. & Vines, R.D. 2004. The CISSP Prep guide. Mastering the CISSP and ISSEP exams. 2. painos. Wiley Publishing Inc. USA. 1024 s.

Kyrölä, Tuija. 2001. Esimies ja tietoriskien hallinta. Helsinki. WSOY. 307 s.

Liebowitz, Jay. 2006. Strategic intelligence – Business intelligence, Competitive intelligence, and knowledge management. Boca Raton, Florida, USA. Auerbach Publications. 223 s.

Lukka, K. 1999. Case/field-tutkimuksen erilaiset lähestymistavat laskentatoimessa. Teoksessa Hookana-Turunen, Heli (toim.) Tutkija, opettaja, akateeminen vaikuttaja ja käytännön toimija. Professori Reino Majala 65 vuotta. Turun kauppakorkeakoulun julkaisuja, C-1:1999, ss. 129-150.

Manyika, J., Chui, M., Bisson, P., Woetzel, J., Dobbs, R., Bughin, J. & Aharon, D. 2015. The Internet of Things: Mapping the Value Beyond the Hype. McKinsey Global Institute.

Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Jyväskylä. Gummerus Kirjapaino Oy. 318 s.

Nonaka, I. & Takeuchi, H. 1995. The knowledge-creating company: How Japanese companies create the dynamics of innovation. Oxford University Press. 284 s.

Olkkonen, T. 1994. Johdatus teollisuustalouden tutkimustyöhön. Toinen painos. Espoo. Teknillinen korkeakoulu. 143 s.

Ozier, Will. 2004. Risk analysis and assessment. Tipton, H & Krause, M. (toim.) Information security handbook. 5. painos. Boca Raton, CRC Press. ss. 795-820.

Peltier, T.R., Peltier, J. & Blackley, J. 2005. Information security fundamentals. CRC Press LLC, Boca Raton. 262 s.

Reddy, Aala Santhosh. 2014. Reaping the Benefits of the Internet of Things. Teaneck, New Jearsey, USA. Cognizant, Cognizant Reports. 9 s.

Roman, R., Najera, P. & Lopez, J. 2011. Securing the internet of things. IEEE Computer security. Vol. 44. Is. 9. ss. 51-58.

Saaranen-Kauppinen A. & Puusniekka A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto [verkkojulkaisu]. Tampere: Yhteiskuntatieteellinen tietoarkisto [ylläpitäjä ja tuottaja]. Viitattu 26.1.2016. Saatavissa: http://www.fsd.uta.fi/menetelmaopetus/kvali/L6_3_3.html

Sharp, D.E. 2004. Information security in the enterprise. Tipton, H & Krause, M. (toim.) Information security handbook. 5. painos. Boca Raton, CRC Press. ss. 767-777.

Sicari, S., Rizzardi, A., Griego, L.A. & Coen-Porisini, A. 2015. Security, Privacy and Trust in Internet of Things: The Road Ahead. Computer networks. Vol. 76. ss. 146-164.

Sorebo, Gib. 2015. Managing the risk of the internet of things. Control Engineering. CFE Media, Barrington.

Stoneburner, G., Goguen, A. & Feringa, A. 2002. Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology. Special Publication 800-30. 54 s.

Ståhle, P. & Grönroos, M. 1999. Knowledge management – tietopääoma yrityksen kilpailutekijänä. 2. painos. Porvoo. WSOY. 218 s.

Sydänmaanlakka, Pentti, K. 2007. Älykäs organisaatio. 8. painos. Helsinki. Talentum Media Oy. 299 s.

Tan, L. & Wang, N. 2010. Future Internet: The Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 2010. ss. 376-380.

Thierauf, Robert, J. 2001. Effective business intelligence systems. Westport. Connecticut. USA. Quorum Books. 330 s.

Tipton, H. & Krause, M. 2004. Information security management handbook. 5. painos. CRC Press, Boca Raton. 2036 s.

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta. Valtiovarainministeriö.

VAHTI 7/2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtiovarainministeriö.

VAHTI 8/2008. Valtionhallinnon tietoturvasanasto. Valtiovarainministeriö.

Vermesan, O., Friess, P., Guillemin, P., Gusmeroli, S., Sundmaeker, H., Bassi, A., Jubert, I., Mazura, M., Harrison, M., Eisenhauer, M. & Doody, P. 2011. Internet of Things Strategic Research Roadmap. Toim. Vermesan, O. & Friess, P. Internet of Things - Global Technological and Societal Trends. Aalborg, Denmark 2011. River Publishers. ss. 9-52.

Watson, D., Piette, M., Sezgen, O. & Motegi, N. 2004. Machine to Machine (M2M) Technology in Demand Responsive Commercial Buildings. Proceedings of ACEEE Summer Study on Energy Efficiency in Buildings. Pacific Grove, California, USA. ss. 1-14.

Weber, Rolf, H. 2010. Internet of things – New security and privacy challenges. Computer Law & Security Report. Vol. 26. ss. 23-30.

Whitman, M.E. 2003. Enemy at the gates: Threats to information security. Communications of the ACM. Vol. 48. No. 8. ss. 91-96.

Whitman, M.E. & Mattord, H. J. 2005. Principles of information security. 2. painos. USA, Thomson Learning. 576 s.

Wood, C.C & Saari, J. 1992. A Strategy for developing information security documents. Information Systems Security. Vol. 1. Is. 2. ss. 71-78.

Wu, M., Lu, T-J., Ling, F-Y., Sun, J. & Du, H-Y. 2010. Research on the Architecture of Internet of Things. 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE). IEEE. ss. 484-487.

Xu, L.D., He, W. & Li, S. 2014. Internet of things in industries: A survey. IEEE Transactions on industrial informatics. Vol. 10. Is. 4. ss. 2233-2243.

LIITE 1: HAASTATTELURUNKO

HAASTATELTAVIEN TAUSTAT:

- Kuka olet ja mikä roolisi on yrityksessä?
- Millaisia vastuualueita sinulla on?
- Kauanko olet ollut yrityksessä?
- Kauanko olet työskennellyt tietoturvallisuuden parissa?
- Kauanko olet työskennellyt esineiden internetin parissa?

HAASTATTELURUNKO A (haastattelut 1-3):

1. Mitä tietoturvauhkia näet esineiden internetissä?

   Mitkä näistä ovat kaikkein vakavimpia?

   Miksi?
2. Mitä tietoturvauhkia älyauto on tuonut tullessaan?
3. Mitä tietoturvauhkia näet kategoriassa (havainnointi/siirto/sovellus)?
4. Vaarantaako uhka tiedon luottamuksellisuuden, eheyden tai saatavuuden? Tai useamman näistä?

   Miksi?
5. Mitkä näistä uhista koet vakavimmiksi?

   Miksi?
6. Minkä arvosanan asteikolla 1-5 antaisit uhalle sen vaikutuksesta?

   Miksi?
7. Minkä arvosanan asteikolla 1-5 antaisit uhalle sen todennäköisyydestä?

   Miksi?
8. Oliko kysymyksiin mielekästä vastata?

   Miten kysymyksiä voisi parantaa?
9. Oliko kysymyksiin helppoa vastata?

   Mikä oli vaikeaa?
10. Miten haastattelua voisi parantaa entisestään?
11. Tuleeko sinulle mieleen jotain tämän diplomityön kannalta merkityksellistä, jota et päässyt vielä sanomaan?

HAASTATTELURUNKO B (haastattelut 4-6):

1. Mitä tietoturvauhkia näet kategoriassa (havainnointi/siirto/sovellus)?
2. Vaarantaako uhka tiedon luottamuksellisuuden, eheyden tai saatavuuden? Tai useamman näistä?

   Miksi?
3. Mitkä näistä uhista koet vakavimmiksi?

   Miksi?

Edellisissä haastatteluissa tunnistetut tietoturvariskit:

4. Onko sinulla lisättävää näihin uhkiin? Tuleeko sinulle mieleen jokin uhka, mitä ei tullut vielä esille, mutta on merkittävä esineiden internetissä?
5. Millaisia hallintakeinoja näille uhilla on olemassa?

   Onko yhdelle uhalle useampi tapa hallita sitä vai vain yksi?
6. Millainen on tehokas hallintakeino?

   Miksi?
7. Mitkä hallintakeinot ovat tehokkaita kyseessä olevan uhan kannalta? Miksi on/ei ole tehokas?

   Miksi tämä toimii/ei toimi?
8. Miten kyseessä oleva hallintakeino pienentää uhkaa?
9. Millainen panostus hallintakeinon toteuttaminen on?
10. Tuleeko sinulle mieleen jotain tämän diplomityön kannalta merkityksellistä, jota et päässyt vielä sanomaan?